Council of the European Union

Brussels, 26 June 2026
(OR. en)

11158/26
ADD 2

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
HYBRID 85
CT 86

COVER NOTE

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.:	SWD(2026) 580 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document 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 SWD(2026) 580 final.

Encl.: SWD(2026) 580 final

EUROPEAN
COMMISSION

Brussels, 24.6.2026
SWD(2026) 580 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

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

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

Table of contents

Glossary

Term or acronym	Meaning or definition
AIRPOL	Law enforcement network in the European aviation sector
AMLA	Authority for Anti-Money Laundering and Countering the Financing of Terrorism
AP	Analysis Project
ATLAS	European Cybersecurity Atlas
CAAR	Consolidated Annual Activity Report
CEPOL	European Union Agency for Law Enforcement Training
CODIS	Combined DNA Index System
COSI	Standing Committee on Operational Cooperation on Internal Security
DSC	Data Subject Categorisation
EAS	Europol Analysis System
EBCG Regulation	Regulation (EU) 2019/1896 on the European Border and Coast Guard Agency
ECB	European Central Bank
ECCC	European Cybersecurity Competence Centre
EDPS	European Data Protection Supervisor
EEAS	European External Action Service

EFECC	European Financial and Economic Crime Centre
EIFS	European In-Flight Security Officer Network
EIGE	European Institute for Gender Equality
EIS	Europol Information System
ELA	European Labour Authority
EMPACT	European Multidisciplinary Platform Against Criminal Threats
ENISA	European Union Agency for Cybersecurity
ENU	Europol National Unit
EPPO	European Public Prosecutor's Office
EPRIS	European Police Records Index System
ER	Regulation (EU) 2016/794 ("Europol Regulation")
EUAA	European Union Agency for Asylum
EUCARIS	European Car and Driving Licence Information System
EUDA	European Union Drugs Agency
EU-SOCTA	European Union Serious and Organised Crime Threat Assessment
Eurojust	European Union Agency for Criminal Justice Cooperation
Eurojust Regulation	Regulation (EU) 2018/1727
Europol	European Union Agency for Law Enforcement Cooperation

Europol Regulation	Regulation (EU) 2016/794
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
FEPORT	Federation of European Private Port Companies and Terminals
FRA	European Union Agency for Fundamental Rights
Frontex	European Border and Coast Guard Agency
HRSN	High Risk Security Network
Interpol	International Criminal Police Organization
IOCTA	Internet Organised Crime Threat Assessment
JAD	Joint Action Days
JHA	Justice and Home Affairs
JIT	Joint Investigation Team
JOAC	Joint Operational Analysis Case Platform
LED	Law Enforcement Directive
LEWP	Law Enforcement Working Party
MAOC (N)	Maritime Analysis and Operations Centre (Narcotics)
OLAF	European Anti-Fraud Office
OSINT	Open-Source Intelligence

OTF	Operational Task Forces
PD	Programming Document
QUEST	Querying Europol Systems
RAILPOL	European Association of Railway Police Forces
REFIT	Commission's Regulatory Fitness and Performance Programme
SDG	Sustainable Development Goal
SIENA	Secure Information Exchange Network Application
SPoC	Single Points of Contact
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UMF	Unform Messaging Format

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

The EU is entering a **new security era** marked by rapid and lasting change. The assumptions that shaped Europe's internal security framework even a decade ago are increasingly being overtaken by a reality in which threats evolve faster, operate across borders by default, and unfold across highly interconnected digital, economic, and societal systems. At the same time, serious and organised crime, terrorism, cybercrime, and hybrid threats increasingly converge, combining criminal activity, cybercrime operations, and economic interference. Their effects ripple across the EU, threatening economic stability, straining institutional resilience, and eroding public trust. Geopolitical instability, including Russia's war of aggression against Ukraine, has further amplified these risks.

As emphasised by the European Council in June 2025, *"serious and organised crime, and terrorism, radicalisation and violent extremism, both online and offline,* ***represent a major threat to European citizens and the security of Member States****"*[1], requiring the mobilisation of all relevant instruments at both national and Union level. Their impact reaches beyond security alone, affecting citizens' sense of safety and confidence in the EU's ability to protect them. This concern is tangible, with 64% of EU citizens saying they are worried about the EU's security in the coming years[2].

This evolving threat landscape unfolds within an area without internal frontiers, where free movement is a defining strength of the EU and where preparedness must match the scale and fluidity of cross-border threats. In such a space, security cannot be ensured by Member States acting alone. Europe's security architecture therefore combines action within national jurisdictions with coordination at Union level, where information can be brought together, cross-border connections identified, and common responses enabled[3]. This allows threats to be addressed more effectively and at the right scale. This architecture relies on a broader ecosystem of EU bodies and agencies operating across different stages of the security and criminal justice chain. Within this framework, Europol supports criminal intelligence analysis, operational coordination and information exchange between law enforcement authorities. Eurojust facilitates judicial cooperation and coordination between prosecutors and judicial authorities. The EPPO investigates and prosecutes criminal offences affecting the financial interests of the Union, while OLAF conducts administrative investigations into fraud, corruption and other irregularities affecting the EU budget. Frontex supports border management and contributes to situational awareness at the external borders, including in relation to cross-border crime. Europol increasingly operates in close interaction with these actors, notably through information exchange, analytical support, operational coordination and cross-system cooperation.

These dynamics are reflected in Europol's 2025 EU Serious and Organised Crime Threat Assessment[4], which identifies a **fundamental transformation in the nature of crime**. Criminal networks[5] are more resilient, technologically enabled, and transnational than ever

---

[1] European Council, Conclusions, 26-27 June 2025, EUCO 12/25, para. 41.
[2] Flash Eurobarometer FL550: EU Challenges and Priorities.
[3] Articles 67(3), 87(1), and 88(1) TFEU establish the Union's competence to support and strengthen cooperation between Member States' law enforcement authorities, including through Europol.
[4] Europol (2025) European Union Serious and Organised Crime Threat Assessment (EU-SOCTA).
[5] Europol (2024), Decoding the EU's most threatening criminal networks.

before. They operate simultaneously across multiple jurisdictions and rely extensively on digital infrastructures, encryption, financial systems, and emerging technologies (for example cryptocurrencies or anonymisation tools) to organise, expand, and conceal their activities. Digitalisation has accelerated the scale, reach, and operational sophistication of criminal and terrorist actors. For example, organised crime groups increasingly use encrypted communication platforms, online marketplaces and digital payments to coordinate activities across borders. At the same time, the growing convergence between cybercrime[6], financial crime[7], and terrorism[8] further increases the complexity of the threat environment.

This transformation is driving a change in how security is organised across the EU. Member States are modernising their frameworks and deepening cooperation[9]. More fundamentally, these developments are **reshaping expectations** placed on law enforcement authorities and on the Union's collective capacity to act. No single authority can fully capture or address threats that develop simultaneously across multiple jurisdictions and operational domains.

In response and recognising that internal security is a shared European responsibility, the EU has articulated an ambitious political vision to strengthen its collective security, notably through **ProtectEU – a European Internal Security Strategy[10]**. At the centre of this vision stands Europol, a key instrument of European cooperation in internal security. Established two decades ago to support cooperation between national law enforcement authorities, the agency has progressively evolved into a key operational and analytical hub. By enabling information exchange, criminal intelligence analysis and coordinated action against cross-border crime, Europol helps Member States detect criminal networks, connect intelligence and act collectively against threats that no single national authority could address alone. Over the past 26 years, Europol has evolved from a coordination platform into a central operational and analytical hub at the heart of Europe's law enforcement architecture. By supporting thousands of operations each year and enabling millions of information exchanges, Europol has helped transform fragmented national efforts into a more connected European response.[11]

Europol is today a force multiplier for European security, reflecting a shift from cooperation as an option to **cooperation as a necessity**. This level of integration, once unimaginable, has been enabled through successive legal reinforcements,[12] building on Member States' willingness to pool expertise and capabilities to step up the fight against serious crime and terrorism. In doing so, it gives practical effect to the Treaties' objective of ensuring a high level of security for the EU and its citizens in an area without internal

---

[6] Europol (2024), Internet Organised Crime Threat Assessment (IOCTA) 2024.
ENISA (2025), ENISA Threat Landscape October 2025.
[7] Europol (2023), European Financial and Economic Crime Threat Assessment 2023.
[8] Europol (2025), European Union Terrorism Situation & Trend Report.
[9] For instance, the Netherlands, Belgium, Germany, France, Italy, Spain, Sweden have formed the European coalition to fight Organised crime.
[10] COM (2025) 148 final.
[11] In 2024 alone, Europol supported more than 3 300 operations, enabled over 2 million secure information exchanges, and provided access to its databases nearly 15 million times.
[12] Regulation (EU) 2016/794 was amended in 2022 by Regulation (EU) 2022/991 to address new security threats and in 2025 by Regulation (EU) 2025/2611 to effectively counter migrant smuggling.

frontiers[13]. As its mandate and tools have evolved, Europol has become a central pillar of a more integrated and operational European security architecture.

Yet Europol's success has also raised expectations about what European cooperation can deliver. It has shown that collective action and EU support can extend the reach and effectiveness of national authorities. In particular, the **2022 reform**[14] marked a decisive strengthening of Europol's mandate, addressing urgent operational and legal constraints identified at that time, notably concerning large datasets and cooperation with private parties. However, the operational and technological environment has evolved at a significantly faster pace than anticipated at the time of the 2022 reform, with an exponential increase in multi-source data, growing expectations regarding proactive operational support, and the emergence of more integrated EU security frameworks and cooperation models. Threats that once appeared at the periphery have moved to the forefront, redefining the scale and intensity of the challenges facing the Union[15]. These developments have revealed structural limitations in the current mandate which go beyond the targeted adjustments introduced in 2022.

This acceleration calls for safeguarding Europol's ability to operate effectively in the face of new threats. This ambition lies at the heart of the Union's political priorities. In her **Political Guidelines, President von der Leyen** called for making Europol "a truly operational police agency", signalling a clear commitment to equip the Union with the capabilities required to respond to a rapidly evolving threat environment.

This impact assessment therefore examines how Europol's legal framework, capabilities and resources need to evolve to ensure the Union remains able to address emerging security challenges effectively, with a stronger focus on speed, integration, and operational effectiveness. As technology redefines the nature of security itself, it is essential to put in place a robust and future-proof framework that enables Europol to respond to evolving threats, in close coordination with all relevant Union bodies and agencies, while remaining firmly grounded in the Union's values and trusted by its citizens, including by maintaining a high level of data protection at Europol.

This assessment takes place within a **broader effort to strengthen the Union's overall security architecture** as outlined in ProtectEU. In this context, several legislative and policy initiatives are being advanced to reinforce the EU's response to serious and organised crime and terrorism. These include the recently adopted proposal establishing EU-wide rules against the trafficking of illicit firearms[16] and the forthcoming proposal establishing new EU rules to fight organised crime[17]. At the same time, a number of operational and strategic initiatives have been put forward to support Member States in

[13] Article 88 TFEU defines Europol's mission to support and strengthen cooperation between Member States' law enforcement authorities in preventing and combating serious cross-border crime and terrorism.
[14] Regulation (EU) 2022/991 amending Regulation (EU) 2016/794.
[15] The prominence of technology-related drivers has increased significantly in Europol threat assessments. While references to AI and digital technologies in Europol's EU-SOCTA 2021 were largely forward-looking, Europol's EU-SOCTA 2025 places these technologies at the core of its analysis across multiple threat areas.
[16] 2026/0059 (COD).
[17] Commission work programme 2026 – COM (2025) 870 final.

addressing evolving threats, including the new EU Drug Strategy[18] and Action Plan against drug trafficking[19], and the Agenda to prevent and counter terrorism[20].

It also contributes to improving the effectiveness of the **EU's unique ecosystem of specialised bodies and agencies,** whose mandates are being revised[21] to reflect evolving operational demands. Frontex[22], Europol, Eurojust[23], and the EPPO[24] each fulfil distinct but complementary roles across the security and criminal justice continuum. Ensuring seamless cooperation and information exchange between them is essential for a more integrated and effective European response. In practice, these interactions increasingly require continuous operational coordination and interoperable information flows across the different stages of detection, intelligence development, investigation, prosecution and operational follow-up. This includes, for example, Europol's analytical support to cross-border investigations coordinated by Eurojust, cooperation with the EPPO in complex financial and organised crime investigations, exchanges with OLAF in relation to fraud patterns affecting the EU budget and support to Frontex regarding criminal intelligence linked to migrant smuggling, trafficking in human beings and other cross-border criminal activities. Closer cooperation and information exchange between relevant EU bodies and agencies is also an integral part of the comprehensive review of the EU's anti-fraud architecture (AFA) to strengthen oversight and accountability[25].

The revision of Europol's framework also takes place in parallel with the revision of Chapter IX of the **EU legal framework on data protection for EU institutions, bodies, offices and agencies (EUDPR)[26]**. This provides an opportunity to ensure full coherence and alignment between Europol's evolving operational mandate and the EU data protection framework[27].

In this evolving landscape, ensuring that Europol remains capable of supporting a strong and integrated European response to security threats **remains strategically important for the Union**. It also provides an opportunity to ensure greater legal coherence across the broader EU internal security framework, including ongoing reforms affecting information

---

[18] COM(2025) 743 final.
[19] COM (2025) 744 final.
[20] COM(2026) 101 final.
[21] In accordance with the Commission work programme 2026.
[22] The European Border and Coast Guard Agency (EBCGA), established by Regulation (EU) 2019/1896, is responsible for the implementation of European Integrated Border Management at the EU's external borders.
[23] The EU Agency for Criminal Justice Cooperation (Eurojust), established by Regulation (EU) 2018/1727, provides support to prosecutors and judges, notably by supporting Joint Investigation Teams and facilitating cases involving a European Investigation Order.
[24] The European Public Prosecutor's Office (the EPPO), established by Council Regulation (EU) 2017/1939, is the independent office responsible for investigating and prosecuting crimes against the financial interests of the EU.
[25] The Commission work programme 2026 announced a comprehensive review of the EU's anti-fraud architecture, building on the July 2025 Commission White Paper (COM(2025) 546 final).
[26] In particular, Chapter IX of Regulation 2018/1725.
[27] The objective is to streamline procedures and clarify roles, while fully maintaining a high level of data protection in line with EU standards. In doing so, the overall reform does not merely preserve existing standards but also simplifies the data protection framework by removing fragmentation, which should ensure a unified regime across EU law enforcement and criminal justice authorities and facilitate information sharing between them.

exchange, interoperability, anti-fraud cooperation and operational coordination between Union bodies and agencies.

2. PROBLEM DEFINITION

In today's security environment, effective cooperation between law enforcement authorities and **strong EU-level coordination** have become essential to complement and reinforce Member States' efforts.

The importance of strong European cooperation is reflected in the European Police Chiefs Convention of 2023[28] and the joint call by European Police Chiefs[29] in 2025 to further strengthen Europol's role.

Despite its strengthened mandate, Europol is **not fully equipped to fulfil its mission in this evolving environment.** As highlighted in the Commission report pursuant to Article 68(3) of the Europol Regulation[30] and in the evaluation of Europol[31], the Agency faces legal, operational, and structural constraints that limit its ability to provide timely, comprehensive, and actionable support to Member States. **Persistent information gaps** hinder the development of a complete criminal intelligence picture of cross-border threats. **Uneven and fragmented operational cooperation** and coordination with Member States limit the added value of Europol's support for the action of national authorities on the ground. **Limitations in technical capabilities**, specialised expertise, and preparedness reduce the ability to respond effectively to increasingly sophisticated and technologically enabled criminal activity. Together, these constraints reduce Europol's operational effectiveness and its capacity to deliver its full added value.

As a result, a **structural gap** is widening between the Union's security ambitions and Europol's ability to fully deliver on its mission in practice. The scale, speed, and sophistication of emerging threats are placing demands on Europol that its current framework struggles to meet. When criminal intelligence cannot be fully connected and operational responses cannot be coordinated in time, critical opportunities to detect and disrupt cross-border criminal activity are lost, weakening the EU's ability to respond.

2.1. What are the problems?

2.1.1 Problem 1: Europol and national authorities face persistent information gaps when investigating cross-border crimes and identifying threats.

[28] Future of policing main focus as police chiefs meet at Europol | Europol.
[29] European Police Chiefs (20 April 2025) Joint Statement by the European Police Chiefs on the Future Development of Europol, Kraków.
[30] COM(2025) 752 final.
[31] See Annex 7.

Serious and organised crime, terrorism and hybrid threats increasingly operate across jurisdictions and digital environments. Effective investigations therefore depend on the ability of national authorities and Europol to access and connect relevant information.

However, Member States' law enforcement agencies do not share sufficient relevant data with Europol. Therefore, **information available at EU level remains uneven and incomplete**[32], affecting Europol's analytical capabilities and leaving investigators without a complete picture of criminal networks operating across borders. As a result, parallel investigations may take place without awareness of related cases in other Member States, and links between suspects, criminal activities or financial flows may remain undetected. This reduces the effectiveness of cross-border investigations and **limits Europol's ability to identify connections between cases**, delaying the detection of organised crime structures and weakening the capacity to anticipate evolving criminal threats.

Data contributions via the Secure Information Exchange Network Application[33] (SIENA) and the Europol Information System[34] (EIS) vary significantly, with a limited number of Member States providing a disproportionate share of operational data, while contributions from other Member States are limited. This uneven distribution creates **structural blind spots** that can be exploited by cross-border criminal networks. In addition, even where data are shared, they are often incomplete or **lack key identifiers**, that is, are not provided in the structured format that would allow automatic comparison of records for reliable cross-matching[35]. Investigators are often confronted with inconsistent data quality, or with data that is collected or stored in different formats from their own and hence cannot be used in the investigators' own case management systems without manual processing. These differences cost time and reduce usability, directly affecting **national investigations**.

Moreover, Europol faces **operational constraints in processing large datasets** relevant for cross-border investigations. In particular, the application of Data Subject Categorisation (DSC) under the Europol Regulation[36] delays the intake and analysis of large volumes of data, as the categorisation of large or unstructured datasets often requires manual intervention and additional proportionality assessments. In time-sensitive

[32] Key data relating to suspects, financial flows, communication identifiers, travel movements or digital accounts may be held by different Member States without being connected at EU level.
[33] In 2025, the share of SIENA messages exchanged by Member States where Europol was involved varied from 24% to 56% across Member States. For more information on SIENA, see Annex 8.
[34] As of 31 December 2025, around 90% of the objects stored in the EIS had been introduced by Member States representing around 25% of the EU population, while Member States representing more than 50% of the EU population contributed to less than 5% of the objects shared by EU Member States. For more information on the EIS, see Annex 8.
[35] In 2025, overall, 18% of messages received by Europol contained structured information, varying across Member States from 0.1% to 21%. For more information on cross-checking, see Annex 8.
[36] Under Union law, both Europol and Member States must perform DSC for their own processing of personal data in criminal investigations, regardless of whether the data are subsequently transferred to Europol. However, the legal requirements applicable to Europol differ from those applied by Member States, Eurojust or the EPPO. Under the Europol Regulation, Europol must classify individuals whose personal data appear in a dataset into categories defined in Annex II of that Regulation (e.g. suspects, associates, victims or witnesses) before the data can be fully processed.

investigations, this limits Europol's ability to rapidly identify links between suspects, detect emerging criminal networks and provide timely operational support[37].

2.1.2 Problem 2: Europol's operational support remains limited and fragmented

Crime is borderless and the most threatening criminal networks in the EU affect all Member States[38]. Despite its central role in enabling a necessary cross-border response through EU-level law enforcement cooperation, Europol's operational support to Member States – including through cooperation with partners, in particular EU bodies and agencies – remains **limited, fragmented and uneven.**

In particular, cooperation between Europol and other EU bodies and agencies is marked by weak information exchange and insufficient institutionalisation, which limits the potential for timely and comprehensive EU-level responses to cross-border crime.

Across Member States, engagement with Europol[39] varies significantly in terms of the frequency of operational requests, participation in analytical projects and operational task forces, and use of Europol's information systems[40]. The efficient and comprehensive use of Europol's support often depends on national law enforcement agencies' knowledge about the available services and their possible added value for a given investigation. As a result, Europol's operational support, including analytical products, criminal intelligence development and operational coordination, is not always utilised in a consistent and timely manner in ongoing investigations[41]. The Agency's capabilities are therefore not always deployed to their full potential in support of national authorities dealing with serious and organised crime with a cross-border dimension. This significantly affects the overall effectiveness of EU-level support for complex cross-border investigations.

At the same time, national law enforcement authorities across the Union remain **unevenly equipped** with the advanced specialised and technical expertise required to address increasingly technology-enabled forms of crime. While Member States continue to

---

[37] Section (3) on criminal investigations of the Commission report evaluating the operational impact of Regulation (EU) 2022/991, adopted pursuant to Article 68(3) of Regulation (EU) 2016/794 highlights that Europol "cannot process, nor even store, the personal data of individuals who do not fall under [the relevant] categories". This requirement creates a significant administrative and analytical burden in practice, particularly when handling large or unstructured datasets originating from multiple sources. Such data often do not easily correspond to predefined categories, complicating the identification of relevant data subjects and potentially slowing the progress of investigations. As a result, the intake and analysis of large datasets may be delayed at critical early stages of investigations, limiting Europol's ability to identify relevant individuals, detect connections between cases and conduct analytical work on bulk data, including at the request of Member States.

[38] Europol (2024) Decoding the EU's most threatening criminal networks, p. 44.

[39] For instance, only one of 23 Europol Member States which responded to the targeted survey for national law enforcement authorities reported having received more than five requests by Europol to initiate, conduct or coordinate a criminal investigation under Article 6 ER. See Annex [No], Study supporting the evaluation and the impact assessment of the Europol Regulation.

[40] In 2025, more than 90% of the searches carried by EU Member States in Europol data had been carried out by Member States representing less than 20% of the EU population.

[41] ICF (March 2026), Draft Final Report of the Study supporting the evaluation and the impact assessment of the Europol Regulation, Figure 35 and Questions 60-69 dedicated to Europol's operational centres.

strengthen their capabilities, tackling these threats increasingly requires highly specialised tools, expertise and analytical capacities that are costly to develop and maintain at national level. This has led to growing reliance on Europol's specialised technical[42] and innovation[43] support, including training and operational assistance in areas such as digital forensics, artificial intelligence, and cryptocurrency investigations[44]. Demand for such support continues to grow faster than Europol's current ability to provide it, limiting Europol's ability to respond effectively to the operational needs across the Union[45]. As a result, Europol cannot always scale its support in line with the increasing operational demands from Member States, leaving capability gaps at EU level in areas where collective support would be most efficient.

Operational support limitations also stem from and extend to cooperation with **relevant EU bodies and agencies** responsible for preventing and combating cross-border crime within their respective mandates.

Since the **European Public Prosecutor's Office** (EPPO)[46] became operational in 2021, Europol and the EPPO have significantly strengthened their operational cooperation on complex cross-border investigations affecting the Union's financial interests.[47] Over recent years, the growing scale and complexity of EPPO investigations have increased demand for Europol's analytical support, including cross-checking operational data against Europol databases, identifying links across cases, and enriching them[48]. However, the current legal framework governing the exchange and use of operational information between Europol and the EPPO limits the extent of the support Europol can provide, including by analysing relevant datasets[49] and identifying connections between cases. At

---

[42] ICF (March 2026) Draft Final Report of the Study supporting the evaluation and the impact assessment of the Europol Regulation, interviews with national authorities and Europol .

[43] For example, the number of operations supported by the Europol Innovation Lab more than doubled between 2024 and 2025.

[44] Cybersecurity skills shortages further lead to enhanced cyber inequity, creating systemic exposure for law enforcement authorities and the digital infrastructures they rely on. See, for instance, WEF_Global_Cybersecurity_Outlook_2026.pdf.

[45] 87% of respondents mentioned specialised technical skills as an area where Europol should play a stronger role in training and capacity building. See Figure 70, Study supporting the evaluation and the impact assessment of the Europol Regulation. Furthermore, 86% of respondents indicated there are areas where Europol's training offer dedicated to specialised skills should be expanded, see Figure 71, ibid.

[46] In accordance with the Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the [EPPO], the EPPO is responsible for investigating, prosecuting and bringing to judgment the perpetrators of, and accomplices to, criminal offences affecting the financial interests of the Union which are provided for in Directive (EU) 2017/1371.

[47] Article 20a(2) of the Europol Regulation provides that "Europol shall support the investigations of the EPPO and cooperate with it, by providing information and analytical support". Europol supported six EPPO cases in 2021, 28 cases in 2022, 47 cases in 2023 and 83 cases in 2024.

[48] Europol's European Financial and Economic Crime Centre (EFECC) provides specialised analytical support. EPPO estimates for the period 2028-2034 foresee substantial support needs from Europol, including data cross-checks against Europol databases (600-1200 cases), operational analytical support (500-1200 investigations), digital forensics support (80-150 cases), and operational deployments (100-250 investigations).

[49] In this context, it may be noted that the Commission proposal to amend Regulation (EU) No 904/2010 on administrative cooperation in the field of VAT envisages facilitating access for the EPPO and the European

the same time, large volumes of operational data held by the EPPO[50] cannot always be effectively used by Europol for its activities due to mandate limitations. This reduces Europol's ability to support the investigations conducted by national law enforcement authorities and provide them with comprehensive analytical support.

Cooperation between Europol and **Eurojust** also remains limited in practice, particularly due to the very limited exchange of operational information between the two agencies[51]. As a result, Europol receives only a very limited amount of information from Eurojust, constraining its ability to detect links between cases handled by judicial authorities and those analysed within Europol's operational and analytical activities. In addition, gaps persist in the EU-level support available to national authorities seeking to obtain electronic evidence in investigations today,[52] as there is currently no stable and structured EU-level framework for operational cooperation between Europol and Eurojust to support Member States in this regard[53].

More broadly, structured EU-level cooperation in support of investigations into cross-border crime remains uneven across the EU's internal security architecture. Exchanges of information between Europol and other relevant EU actors, including Frontex in the areas of migrant smuggling and trafficking in human beings,[54] the Anti-Money Laundering Authority (AMLA) in financial crime[55], and EU cybersecurity actors, such as the EU Agency for Cybersecurity (ENISA),[56] CERT-EU and the European Cybersecurity

---

Anti-Fraud Office (OLAF) to certain VAT information for the purposes of investigating offences affecting the Union's financial interests (Proposal for a Council Regulation, COM(2025) 685 final). In light of Europol's strengthened role in supporting EPPO investigations, the possible extension of access to similar information for Europol could also be considered.

[50] The EPPO's Case Management System contains rapidly increasing volumes of operational data. For example, approximately 1 406 terabytes of data are stored in relation to three investigations alone, illustrating the scale of data potentially relevant for operational analysis and cross-case link detection.

[51] Both the Europol Regulation (Article 21) and the Eurojust Regulation (Article 49) provide for indirect information exchange between the two agencies on the basis of a hit/no-hit system. In practice, exchanges have remained minimal. Between May 2023 and August 2025, Europol sent 108 SIENA messages to Eurojust containing 2 081 entities for link detection, resulting in eight hits at Eurojust, none of operational relevance to Europol.

[52] According to the European Commission, "more than half of all investigations today involve a cross-border request to access electronic evidence", i.e., "data in electronic form that are relevant in investigating and prosecuting criminal offences". Notably, "electronic evidence is needed in around 85% of criminal investigations, and in two-thirds of these investigations there is a need to request evidence from online service providers based in another jurisdiction. The number of requests to the main online service providers grew by 70% in the period between 2013 and 2016", Frequently Asked Questions: New EU rules to obtain electronic evidence Brussels, 17 April 2018.

[53] Since 2017, Europol and Eurojust have jointly supported EU law enforcement and judicial authorities in obtaining electronic evidence from service providers located in other jurisdictions through the SIRIUS Project. The initiative provided operational guidance, specialised training, investigative tools and a platform facilitating exchanges between authorities and service providers. The SIRIUS Project has been funded by the European Commission's Service for Foreign Policy Instruments (FPI).

[54] Improvements in the exchange of operational information between Europol and Frontex are addressed in the impact assessment for the upcoming revision of the EBCG Regulation.

[55] Reciprocal exchange of operational information between AMLA and Europol is currently not foreseen.

[56] ENISA is established under Regulation (EU) 2019/881 (Cybersecurity Act) and plays a central role in EU cybersecurity cooperation. Its mandate was further expanded by Directive (EU) 2022/2555 (NIS2 Directive), which assigns the Agency key tasks in supporting operational cooperation and situational awareness across the Union's cybersecurity architecture.

Competence Centre (ECCC)[57], remain limited, reducing the potential for coordinated responses to cross-border and cyber-enabled crime.

2.2. What are the problem drivers?

2.2.1 Problem 1: Europol and national authorities face persistent information gaps when investigating cross-border crimes and identifying threats.

Driver 1.1: Regulatory, legal and procedural constraints affecting information sharing

Divergent national criminal procedure laws and differing interpretations of necessity and proportionality drive selective and inconsistent information sharing between Member States and Europol. Political sensitivities, historical cooperation patterns and varying levels of trust in Europol's handling of sensitive data (e.g. terrorism, minors, financial crime or migration cases) further reinforce conservative practices among Member States.

As a result, information exchange remains uneven and incomplete, with Member States sometimes limiting or delaying transmission of operational data, even where cooperation would be legally possible and operationally justified. This is reflected in significant variations in Member States' contributions to Europol systems and in the uneven use of information exchange channels.

Driver 1.2: Operational and technical limitations in data automation, integration and standardisation hampering information exchange

Member States' law enforcement IT systems differ significantly in terms of automation, connectivity, and their ability to produce structured, interoperable data. Only a few operate automated data loaders to transmit data to Europol[58], while others rely on manual processes or, in some cases, bypass EU channels altogether. Europol's core systems remain underutilised[59], reducing cross-border visibility and EU-level situational awareness. Therefore, the available statistics point to significant disparities in connectivity and data transmission practices across Member States.

Even where connectivity exists, most operational information is transmitted in unstructured formats requiring manual processing. The lack of common data models, standardised templates and automated workflows slows ingestion, cross-checking and analysis. These technical limitations reduce scalability and prevent near-real-time criminal intelligence production, including for biometric and multimedia data, thereby limiting Europol's analytical capacity and operational added value.

Driver 1.3: Regulatory, legal and procedural constraints affecting data processing

---

[57] SWD(2026) 11 final.
[58] In 2025, only 14 Member States operated data loaders.
[59] For example, in 2025, only 15 Member States allowed their users to perform direct searches in Europol data via a technical application called QUEST. For more information on QUEST, see Annex 8.

Compliance requirements related to data protection rules, in particular regarding DSC[60], operate in practice as structural constraints on information processing.

The requirement to apply DSC *ex ante*, combined with intensive procedural safeguards, slows down or in some cases prevents the timely processing and further handling of data, particularly in fast-moving or data-intensive investigations. Europol experience indicates that the application of DSC to large datasets can require significant time and specialised resources before operational analysis can begin.

While legally robust, these procedural requirements reduce operational agility and delay access to cross-border intelligence. As a consequence, Europol and Member States may face constraints in fully exploiting lawfully available data, even where processing would be operationally necessary and proportionate.

Driver 1.4: Structural and operational shift in the criminal data and information environment

The digital transformation of crime has fundamentally changed the nature and volume of information relevant to criminal investigations. Criminal networks increasingly operate across digital platforms, financial systems and communication infrastructures spanning several jurisdictions, generating large volumes of fragmented operational data held by different authorities. The growing use of technologies such as artificial intelligence further increases the speed, scale and complexity of criminal activity[61].

As a result, effective responses to serious and organised crime increasingly depend on the rapid exchange, correlation and analysis of information across national and EU-level systems. In practice, key elements of an investigation are often dispersed across several Member States and authorities, making it necessary to connect different pieces of information – such as suspects, communication data or financial transactions – in order to detect cross-border criminal networks. However, existing information-sharing mechanisms were largely designed for more limited data volumes and slower operational cycles. They rely mainly on message-based exchanges between authorities, where information is shared case by case rather than analysed collectively across systems. This can make it harder to identify links between investigations and to build a timely and comprehensive EU-level criminal intelligence picture.

2.2.2 Problem 2: Europol's operational support remains limited and fragmented

[60] Data Subject Categorisation (DSC) refers to the requirement under the Europol Regulation to assign each personal data record processed by Europol to a specific category of data subject (such as suspects, convicted persons, potential future offenders, victims, witnesses or other contacts and associates), together with corresponding conditions governing the processing and retention of such data. This categorisation aims to ensure compliance with EU data protection rules but can limit the ability to process certain datasets where the status of individuals cannot be clearly determined at the time the data are received.
[61] The 2025 European Union serious and organised crime threat assessment, (EU-SOCTA 2025).

Driver 2.1: Operational limited awareness of Europol's operational support

Awareness among Member States of the full range of Europol's operational tools, services and capabilities remains uneven[62]. As the use of Europol's operational support is voluntary and initiated at national level[63], national authorities may not always consider Europol's involvement at an early stage of investigations.[64] This results in delayed engagement with the Agency and limits the timely exchange of information, the early identification of cross-border links, and the effective use of Europol's capabilities to support coordinated EU-level responses to serious and organised crime.[65] Available operational data show important differences between Member States in the frequency and timing of requests for Europol operational support.

Driver 2.2: Operational and capability-related constraints limiting the tailoring of Europol's support to national investigative needs

While Europol provides operational support to Member States, the support provided is not always sufficiently tailored to the specific needs[66], legal frameworks and evidentiary requirements of national investigations. As a result, the analytical outputs or information provided by Europol may not always be directly usable in national proceedings. In some cases, national authorities must repeat investigative or analytical steps to produce evidence that complies with national procedural requirements. This creates inefficiencies, increases the workload for national investigators and reduces the overall effectiveness of the operational support provided by Europol.

At the same time, the rapid digitalisation of crime requires investigators to use increasingly specialised tools, technologies and skills, including in areas such as digital forensics, artificial intelligence and cryptocurrency investigations. Europol's current framework limits its ability to develop and provide such tools and specialised training at scale across the Union, constraining its capacity to support technology-enabled investigations. Demand for specialised operational support and advanced analytical capabilities has increased significantly in recent years

---

[62] ICF (March 2026), Draft Final Report of the Study supporting the evaluation and the impact assessment of the Europol Regulation, Annex 10.3.1.

[63] Under the Europol Regulation, Europol may support investigations, coordinate operational actions and participate in Joint Investigation Teams, but it cannot initiate investigations or conduct operational activities without the agreement of the Member States concerned.

[64] Evaluation evidence, from the study supporting the evaluation and impact assessment of the Europol Regulation, indicates that Europol's operational support is often mobilised only at a relatively advanced stage of national investigations.

[65] "Case study evidence on Europol's operational centres confirms that the agency's support often focuses on strengthening ongoing investigations rather than shaping investigative strategies from the outset", ibid.

[66] ICF (March 2026) Study supporting the evaluation and the impact assessment of the Europol Regulation - "Limited timeliness of replies via SIENA" is mentioned as a barrier by 40% of respondents, Figure A7.27, Annex 7. Interviews with national authorities highlighted the time required to obtain analytical outputs from Europol can be significant in cases involving large or technically complex datasets.

Driver 2.3: Limited capacity for systemic modernisation of law enforcement capabilities

In many Member States, organisational, legal, and procurement constraints limit the systematic uptake and scaling of innovation, resulting in fragmented development and uneven deployment of modern investigative tools. Barriers include overlapping responsibilities across national, regional and local authorities, slow procurement processes, and rigid administrative procedures. As a result, innovative solutions are often developed within short-term projects or pilot initiatives but struggle to transition into sustainable operational capabilities deployed at EU level[67]. This creates disparities in operational capabilities across the Union and even stronger reliance on Europol to provide specialised expertise and technical support in cross-border investigations. . Despite the growing demand[68], Europol's role in supporting innovation and specialised capabilities remains limited in scale, constraining its ability to systematically strengthen operational capabilities across Member States[69]. This includes limitations linked to available specialised expertise, technical capacity and scalable operational support resources.

Driver 2.4: Regulatory, legal and operational constraints on information sharing between Europol and the EPPO

The current legal framework does not provide a sufficiently robust basis for systematic operational cooperation between Europol and the EPPO[70]. As a result, cooperation largely relies on *ad hoc* requests and case-by-case arrangements, limiting the systematic mobilisation of Europol's analytical support for EPPO investigations and preventing the full exploitation of complementarities between Europol and the EPPO[71]. In addition, Europol cannot share relevant operational information directly with the EPPO without the

[67] Comparative analysis shows that scaling occurs only where an EU actor combines a clear legal mandate with an operational or coordinating role and sufficient convening power. Where such a mandate is absent, innovation remains locked at pilot level by design, regardless of technical maturity or demonstrated usefulness. Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security R&I (DG HOME, 2025)

[68] See Joint Statement by the European Police Chiefs on the Future Development of Europol. Moreover, the results of the public consultation show strong support for enhancing Europol's technological and innovation capabilities, see the factual summary report registered under Ares(2026)2806442 and published at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Law-enforcement-cooperation-new-Europol-regulation-proposal-/public-consultation_en.

[69] For instance, Europol's Innovation Lab and EU-funded projects run "sandboxes" to experiment with AI algorithms; however, due to data protection constraints, these activities cannot rely on real operational crime data.

[70] The EPPO (November 2025), Note [to DG HOME of the European Commission] on improving the cooperation between the EPPO and Europol. See also ICF (March 2026), Draft Final Report of the Study supporting the evaluation and impact assessment of the Europol Regulation, sub-driver 2.5.3 'Legal and mandate limitations hinder cooperation with EPPO'.

[71] ibid.

consent of the Member State that provided the data[72], which significantly delays access to information relevant for EPPO investigations[73].

Driver 2.5: Weak information exchange and insufficiently institutionalised cooperation between Europol and other EU bodies and agencies

Despite the growing need for seamless cooperation across the EU's internal security architecture[74], crucial information exchange between Europol and other relevant EU bodies and agencies, including Frontex[75], AMLA[76], Eurojust,[77] and OLAF,[78] remains weak. Existing exchanges remain uneven and are often dependent on ad hoc arrangements. This affects the completeness of the EU-level criminal intelligence picture that Europol can provide in support of Member State national authorities. Moreover, broader cooperation between Europol and other relevant EU bodies and agencies, such as Eurojust[79] and ENISA[80], is obstructed by insufficient institutionalisation. This hinders the scope, foreseeability and sustainability of coordinated support benefiting the national authorities of EU Member States.[81]

---

[72] In accordance with the data ownership principle established in Article 19 ER.

[73] Although the EPPO may obtain the same information directly from the Member State concerned under Regulation (EU) 2017/1939, this indirect route duplicates exchanges and may delay access to relevant information, in some cases by up to two months, as indicated by the EPPO at the third thematic expert workshop on the future of Europol, see Annex II.

[74] Communication from the Commission to the European Parliament, the Council, The European economic and social committee and the Committee of the regions on ProtectEU: a European Internal Security Strategy COM(2025) 148 final.

[75] The data on the debriefing interview reports sent by Frontex to Europol, which amounted only to 40 in 2025, exemplifies the overly limited exchange of operational information between the two agencies. The Commission has analysed the problem driver in the impact assessment for the revision of Frontex and may accordingly propose to address the identified shortcomings in Article 90 of the ECBGA Regulation and its implementation through the upcoming legislative initiative on Frontex.

[76] The recent reform of the EU anti-money laundering framework created a new institutional architecture centred on AMLA, but Europol currently lacks a formal interface to exchange operational information with AMLA, which in turn contributes to the fragmentation of the EU financial intelligence landscape. See sub-driver 2.5.4 'Unclear division of roles and weak operational integration between Europol and AMLA', Study supporting the evaluation and impact assessment of the Europol Regulation, interim report, January 2026.

[77] See footnote 51 on the implementation of indirect information exchange on the basis of a hit/no-hit system; 'Implementation challenges' and the box summarising the results of the targeted survey for EU bodies and agencies in Annex 2 of the Impact Assessment for the revision of Eurojust.

[78] See, for instance, European Court of Auditors, Special Report 26/2025 'EU bodies fighting fraud', concluding that, "while the mandates of OLAF, the EPPO, Eurojust and Europol are clearly defined, weaknesses remain in terms of exchange of information". The Commission may propose to strengthen information exchange between OLAF, the EPPO, Eurojust and Europol as part of the upcoming AFA review.

[79] See also the impact assessment for the revision of Eurojust.

[80] The Commission has proposed closer cooperation between Europol and ENISA to improve cybersecurity preparedness and response to ransomware incidents as part of the Cybersecurity Act 2 (COM(2026) 11 final).

[81] For instance, SIRIUS remains a project in nature and thus its mission and sustainability are varying and uncertain as they depend on the types and timings of available EU funding. Notably, further to a change of the funding source (Contribution agreement NDICI THREATS FPI/2024/OPSYS CT NR 700002618 as of 1 January 2025), the beneficiaries of the Project are now the national law enforcement and judicial authorities of third countries, while the dire need expressed by the national authorities of the EU Member States to

2.3. How likely is the problem to persist?

The overall problem is structural and likely to persist, as it is **driven by long-term trends** in the scale, complexity, and digitalisation of serious and organised crime. This will require more timely criminal intelligence, closer operational coordination across Member States and Europol, and access to advanced analytical and technical capabilities. At the same time, Europol's ability to respond effectively will continue to be shaped by its legal framework, technical infrastructure, and available expertise, which cannot evolve automatically in line with operational needs. As cooperation increasingly involves a wider range of actors, including EU bodies and agencies, the need for effective coordination and specialised support at European level will further grow. Without adaptation, these trends are likely to widen the gap between operational needs and Europol's capacity to support Member States effectively.

First, **data-related challenges are expected to intensify sharply** as the volume, speed, and complexity of operational data continue to accelerate. Criminal investigations are increasingly driven by digital evidence, encrypted communications, and data dispersed across multiple jurisdictions and platforms, generating vast and fragmented datasets. At the same time, persistent differences in information sharing practices, limited interoperability, and constraints in processing large and complex datasets will continue to hinder Europol's ability to fully integrate and exploit this information. Without addressing these structural data gaps, Europol risks falling behind the scale and pace at which criminal networks operate, limiting its capacity to generate a complete and timely European criminal intelligence picture and to detect critical cross-border links.

At the same time, Europol's role as an information hub is expected to expand significantly, with increasing volumes of operational data being transmitted from Member States and partners. If existing legal, technical and resource constraints regarding data processing by Europol are not addressed, these growing data flows will place **mounting pressure on Europol's systems and resources**, creating structural bottlenecks. In such a scenario, efforts to improve information sharing and close existing data gaps may yield only limited operational benefit, as the Agency's ability to translate greater data availability into actionable criminal intelligence would remain constrained by existing legal and resource limitations. Rather than strengthening Europol's operational impact, the growing data flows could deepen existing bottlenecks, increasing the burden on the Agency and limiting its ability to deliver timely and effective support in an increasingly demanding security environment.

---

continue relying on the project's knowledge and expertise to successfully obtain critical electronic evidence for criminal investigations and prosecutions (n 53) has remained unmet.

Second, **operational demands on Europol are expected to increase significantly**[82] as the criminal landscape becomes more complex, connected and transnational,[83] requiring faster, more coordinated responses across jurisdictions and actors. Effective action increasingly depends on the ability to rapidly connect information, provide timely analytical and operational support, and facilitate coordinated action across jurisdictions. However, Europol's ability to expand and adapt its operational support is shaped by the scope and modalities defined in its legal framework, which cannot automatically evolve in line with operational needs.

Furthermore, the need for closer cooperation and complementarity between **EU bodies and agencies** will become more critical.[84] Fragmentation and duplication of EU efforts would reduce effectiveness and efficiency, limiting the Union's ability to deliver a coherent and effective operational response to increasingly complex cross-border crime.

Third, **capability gaps are also expected to persist and widen** due to the rapid pace of technological change, including developments in artificial intelligence, digital forensics, and advanced analytics.[85] Criminal networks are early adopters of new technologies, and law enforcement authorities require specialised expertise, advanced analytical tools, and scalable technical infrastructure to respond effectively. However, national innovation capacities and training systems are expected to evolve unevenly due to differing priorities, resources, and organisational constraints. In addition, parallel innovation and development ties up scarce resources. Without stronger coordination at EU level, inefficiencies, disparities in skills[86], technical capabilities, and preparedness across Member States are likely to persist or deepen, limiting the effectiveness of the collective European response.

Taken together, these dynamics suggest that, without intervention, the gap between the complexity of criminal threats and the capacity of Europol and law enforcement authorities to address them effectively **will widen**, with continued implications for the quality of national investigations, the effectiveness of cross-border cooperation and the overall capacity of the Union to respond coherently to serious and organised crime.

---

[82] Even today, there would be thousands more cases where Member States ask for Europol's support if Europol had the capacity to provide that according to the Deputy Director of Europol for Governance, Jürgen Ebner, at "The future of Europol", The Europol Podcast, 18 December 2025. Demand for Europol's services exceeds Europol's current capacity also according to the Study supporting the evaluation and the impact assessment of the Europol Regulation, draft final report, March 2026.

[83] Retooling the police is a priority for a strategic response against the future evolution of organised crime according to the Global Initiative against Transnational Organized Crime (GI-TOC), Intersections: Building blocks of a global strategy against organized crime, p 88. Increasing crime threats and a limited budget decisively contribute to make Europol unable to optimally fulfil its supporting role for the Member States according to the European Police Chiefs.

[84] For instance, in the area of financial crime, while this impact assessment report considers the relationship between Europol and AMLA, GI-TOC has suggested the creation of a *global* financial crime intelligence centre as a priority action to counter the *future* evolution of organised crime, ibid, pp. 80-81.

[85] See the problem definition by the Study supporting the evaluation and the impact assessment of the Europol Regulation, draft final report, March 2026, namely driver 2.2.

[86] Feasibility study on law enforcement training in the EU to strengthen a common EU law enforcement culture, interim report, January 2026.

3. WHY SHOULD THE EU ACT?

3.1. Legal basis

The legal basis of this initiative is Article 88 of the Treaty on the Functioning of the European Union (TFEU), which establishes Europol's mission. In particular, it stipulates that the Agency shall '*support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy*'.

Article 88(2) TFEU empowers the European Parliament and the Council, acting in accordance with the ordinary legislative procedure by means of regulations, to determine Europol's structure, operation, field of action, and tasks.

3.2. Subsidiarity: Necessity of EU action

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

Europol's mandate is to support and strengthen cooperation between Member States' law enforcement authorities in addressing serious and organised crime and terrorism. **These threats increasingly operate across borders**, jurisdictions, and digital environments, requiring coordinated action and the timely exchange and analysis of information at Union level. Member States acting alone cannot ensure the necessary level of coordination, nor can they establish a comprehensive criminal intelligence picture across the Union.

Union action is therefore necessary to provide a common legal framework enabling Europol to effectively support Member States, facilitate cooperation, and strengthen the exchange and analysis of operational information. Moreover, as Europol is a Union agency established by Regulation (EU) 2016/794, any modification of its mandate or functioning can only be achieved through Union legislation. The objectives of this initiative can therefore be better achieved at Union level, in accordance with the principle of subsidiarity.

3.3. Subsidiarity: Added value of EU action

The evaluation of the Europol Regulation (Annex 7) has confirmed that Europol plays a **unique and indispensable role** in supporting Member States in preventing and combating serious and organised crime and terrorism, in particular where these threats have a cross-border dimension. Through its criminal intelligence analysis, operational and technical support to investigations, coordination of cross-border law enforcement actions, and support to joint investigation teams, **Europol expands the reach, speed, and effectiveness of national investigations**. It enables authorities to detect connections between criminal activities across multiple Member States, identify priority targets, and coordinate operational responses, thereby significantly strengthening the Union's collective ability to disrupt criminal networks.

Europol also provides specialised capabilities, expertise, and technological infrastructure that individual Member States could not develop or maintain efficiently on their own.[87] This includes advanced analytical and forensic capacities, the ability to process and analyse very large and complex datasets, and innovation and technical support to address evolving threats. By centralising high-value expertise, tools, and infrastructure at Union level, Europol generates **substantial economies of scale**, reduces duplication of investment, and ensures that all Member States benefit from cutting-edge capabilities, regardless of their size or national resources.

A common Union legal framework ensures that Europol can perform its tasks consistently, effectively, and with full respect for Member States' competences and responsibilities for law enforcement. It also guarantees coherent governance, accountability, and safeguards, including a high level of protection of personal data, thereby strengthening mutual trust and enabling effective operational cooperation. This contributes to ensuring a high level of security across the Union and to protecting the integrity of its internal market[88], democratic institutions, and digital and economic infrastructure.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. General objectives

The general objective of this initiative is to improve the effectiveness of EU-level law enforcement cooperation in preventing and combating serious and organised crime and terrorism, in order to contribute to a high level of internal security in the EU.

In particular, the aim is to enhance Europol's capacity to enable a more complete and timely understanding of criminal threats across the Union and to support their effective detection, disruption and prevention, thereby contributing to the protection of citizens and victims.

4.2. Specific objective

4.2.1 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 focuses on:

- improving the **timeliness and completeness of information exchange**, including reducing delays and gaps in cross-border data sharing;
- ensuring that **relevant information is available and accessible** across Member States and relevant EU bodies and agencies in a consistent and interoperable manner;

[87] See Annex 7: Evaluation of the existing policy and legislative framework pages 120, 124.

[88] https://www.europol.europa.eu/sites/default/files/documents/Europol_report_-_Leveraging_legitimacy_-_How_the_EU_most_threatening_crim_networks_abuse_legal_business_structures.pdf

- improving the **usability of information for operational purposes**, including its structuring, analysis and sharing in an actionable format.

By addressing fragmentation and the under-utilisation of existing tools, this objective will enable the **systematic identification of cross-border links between cases, individuals and criminal networks, including emerging threats, and support more effective operational action**, while maintaining robust data protection and fundamental rights safeguards.

4.2.2. Strengthening Europol's capacity to support law enforcement operational action

This objective aims to ensure that Europol can **provide timely, coordinated and operationally relevant support to cross-border investigations into serious and organised crime and terrorism**. It focuses on:

- enabling **earlier and more consistent involvement of Europol** in cross-border investigations;
- improving the **translation of criminal intelligence into concrete operational results**, including support to coordinated measures;
- strengthening **operational coordination and cooperation with Member States and Union bodies and agencies, in particular the EPPO**, including through a more continuous use of EU-level capabilities.

This will support faster, more coherent and effective investigations, and ensure a more continuous EU-level support across the operational lifecycle, from intelligence to investigation and prosecution.

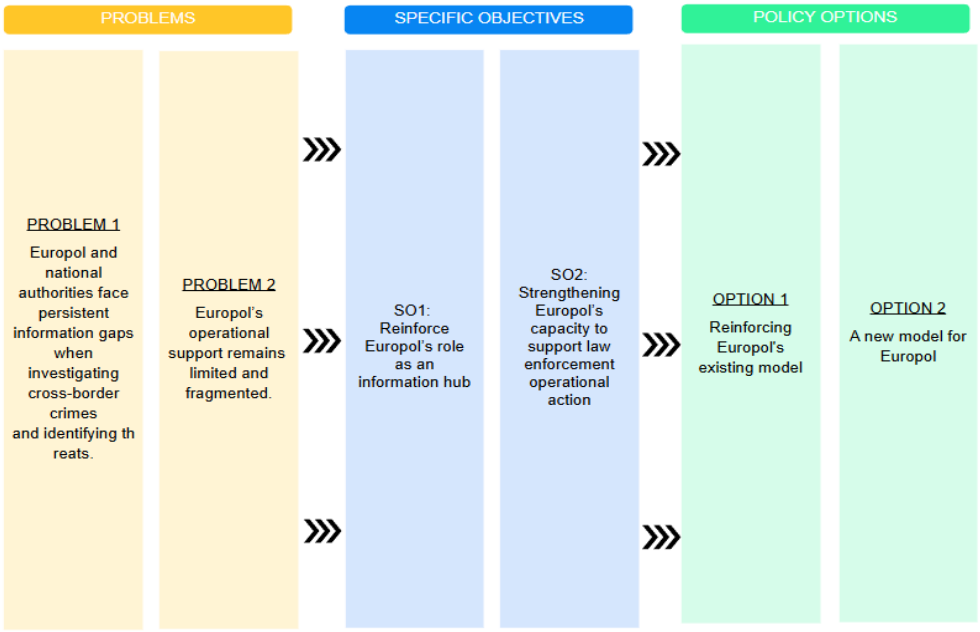


Figure 1: Intervention Logic

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1. What is the baseline from which options are assessed?

The baseline scenario reflects the continuation of the current legal, governance, and operational framework established by Regulation (EU) 2016/794, as amended.

Under this scenario, Europol would continue to support cross-border cooperation, provide criminal intelligence analysis, and contribute to coordinated operational responses, playing a key role in enabling collective action against serious and organised crime and terrorism[89].

Over the period 2027-2037, the operational environment is expected to transform fundamentally, with criminal networks leveraging advanced technologies, scaling their activities across borders with unprecedented speed, and producing volumes of data that challenge the ability of authorities to detect, analyse, and respond effectively[90]. Operational cooperation at Union level will become indispensable, requiring faster, deeper, and more continuous coordination to match the speed, complexity, and reach of evolving threats.

In this evolving environment, Europol would remain a central pillar of the Union's internal security architecture, but the fact that its operational model was conceived for a fundamentally different era would become increasingly evident. As threats grow faster, more data-driven, and more interconnected, Europol's ability to keep pace would be progressively constrained by the limits of its current legal, technical, and organisational framework. While Europol would continue to adapt incrementally, its capacity to **operate at the scale and tempo required** by the evolving threat environment would remain shaped by the limits of its existing legal, technical, and organisational framework.

In terms of **information and criminal intelligence**, Europol would remain the Union's central hub for receiving and analysing criminal data, but the scale and complexity of incoming information would grow far faster than Europol's capacity to fully exploit it. Despite ongoing initiatives to improve connectivity[91] and expand data exchange[92], information flows would remain uneven and incomplete, reflecting persistent disparities in national capabilities and system integration. At the same time, the exponential growth of digital evidence and data-intensive investigations would place mounting pressure on Europol's infrastructure and analytical environment. Increasingly, resources would be absorbed by maintaining and stabilising existing systems, limiting the Agency's ability to scale processing capacity and deploy advanced analytical tools. Without structural change, Europol would face growing difficulty in transforming expanding data volumes into timely

[89] See Annex 7, which presents the evaluation of the Europol Regulation and shows a consistent upward trend.
[90] EU-SOCTA and IOCTA highlight that criminal networks are increasingly digitalised, technologically enabled and transnational, generating growing volumes of data and requiring stronger cross-border operational cooperation.
[91] Examples of Europol's ongoing modernisation efforts include the Information Management and Analysis Capability (IMAC), aimed at strengthening the processing and analysis of criminal information, and the Joint Operational Analysis Capability (JOAC), which enables real-time analytical support to operational activities, including joint investigation teams, operational task forces, and coordinated cross-border investigations.
[92] Considering the EU JHA interoperability roadmap and other developments related to travel information.

and operational criminal intelligence, weakening the Union's ability to detect and disrupt cross-border threats.

Europol's **operational support** would also continue to expand within its existing mandate. Europol would continue to support investigations and coordinated operational activities through analytical contributions, technical expertise, and coordination functions, including support to joint investigation teams, operational task forces, and cooperation with Union bodies and agencies. Europol would also continue to play an important role in facilitating cooperation with international partners, including through closer partnerships with specific countries. However, as operational demands increase in scale and complexity, Europol's ability to provide timely and comprehensive support across all relevant investigations would remain limited by structural factors, including legal and procedural constraints, uneven Member State participation, and limits in the scalability of its analytical and coordination functions. As a result, Europol's operational engagement would remain selective, contributing to uneven levels of operational support across the Union. At the same time, as the mandates and operational activities of other Union actors, notably the EPPO, expand, Europol would be increasingly expected to provide analytical and coordination support, with cooperation continuing to deepen, while remaining hampered by fragmented mandates.

Europol would also continue to provide **specialised expertise and advanced capabilities**, including in digital forensics, decryption, and large-scale data analysis[93], without duplicating those provided by other EU bodies and agencies. Europol's technological role in supporting the Union's response to online threats is also expected to continue expanding in line with existing policy frameworks, including the Digital Services Act[94] and developments under the Cybersecurity Act[95]. This work increasingly involves structured cooperation with private sector actors, including online platforms, financial service providers and technology companies, which play an important role in detecting and reporting criminal activity in the digital environment. These initiatives increasingly rely on Europol's technical and analytical expertise to support the identification and assessment of online risks, including those linked to serious and organised crime, terrorism and illegal content online[96]. Furthermore, the work of Europol's Innovation Lab[97] and the European

[93] For instance, the recommendations of the High-Level Group on access to data and the Commission's roadmap for lawful and effective access to data for law enforcement identify Europol as a key actor in the areas of digital forensics. At the same time, Europol Programming Document 2024-2026 establishes that '*Europol seeks to be at the forefront of law enforcement innovation and research and through its Innovation Lab, it facilitates innovation in the law enforcement community and addresses the risks and opportunities of emerging technologies',* which is strategic objective 5 in that document.

[94] Regulation (EU) 2022/2065.

[95] Regulation (EU) 2019/881.

[96] In particular, Europol's role under Article 18 of Regulation (EU) 2022/2065.

[97] Europol's Innovation Lab, established in 2019, is a collaborative platform within Europol that brings together law enforcement authorities, researchers, technology experts, and industry partners to explore, develop, and test innovative tools, technologies, and methods that help law enforcement agencies across Europe anticipate, prevent, and combat emerging criminal and security threats in an increasingly digital and complex environment. The number of supported operations by the Europol Innovation Lab more than doubled between 2024 and 2025.

Clearing Board[98], and technological developments would contribute to incremental improvements, and Europol would remain a key provider of specialised capabilities that many Member States would not be able to sustain independently. However, the pace of technological change and the increasing sophistication of criminal methodologies would continue to raise operational requirements. Europol's ability to scale advanced capabilities and operationalise emerging technologies would remain shaped by structural constraints, including ICT infrastructure limitations, governance and legal requirements, procurement timelines, and compliance obligations. Legal and procedural safeguards, including narrowly defined mandates governing the use of publicly available information, biometric data, and artificial intelligence tools, would continue to shape the pace and scope of deploying new analytical techniques[99]. In particular, the growing importance of publicly available information and open-source intelligence (OSINT) in criminal investigations would further increase analytical demands on Europol to exploit such data.

In **financial terms**, the baseline scenario assumes the continuation of Europol's current budgetary trajectory under the existing Multiannual Financial Framework, reflecting a no-policy-change scenario. Europol's budget has grown steadily in recent years, increasing from approximately EUR 169 million in 2021 to around EUR 235 million in 2025, reflecting the Agency's gradual expansion of its operational responsibilities and analytical capabilities. Based on this trend, the cumulative Europol budget over the current MFF (2021-2027) is estimated at around EUR 1.5 billion. For the purposes of this impact assessment, baseline projections assume that **Europol's budget would continue to evolve broadly in line with historical trends**, resulting in a projected envelope of approximately **EUR 2.3-2.9 billion** over the following MFF period (2028-2034), depending on whether linear growth or a constant growth rate is assumed[100]. These projections exclude the costs associated with the policy options assessed in this impact assessment and reflect expenditure that would likely be incurred irrespective of the initiative. The budgetary impact of the preferred option should therefore be assessed in addition to the projected baseline envelope.

5.2. Description of the policy options

This Impact Assessment examines two policy options, focusing on the main strategic directions for strengthening Europol's role within the Union's security architecture and presenting those measures contained in the two options that would have the most significant implications. These options are structured around **two distinct policy directions both reflecting an ambitious strengthening of Europol's role**.

Policy Option 1 strengthens Europol's existing mandate and operational model through targeted structural improvements and expanded capabilities, enabling more effective and scalable operations while preserving the current framework.

---

[98] The European Clearing Board is a Europol-coordinated forum where EU Member States and agencies align operational needs and guide the development of innovative law-enforcement technologies.
[99] ICF (March 2026), Draft Final Report of the Study supporting the evaluation and the impact assessment of the Europol Regulation, p.31.
[100] See Annex 3 cost of the preferred option, for more details on the calculation.

Policy Option 2, by contrast, explores a more fundamental evolution of Europol's role, positioning the Agency as an essential Union-level capability for coordinating operations and generating criminal intelligence in response to increasingly complex cross-border threats.

Each policy option comprises a coherent, but not exhaustive, set of measures addressing the specific objectives of strengthening Europol. Some measures represent progressive improvements that could be implemented cumulatively, with Policy Option 2 building on and going beyond elements of Policy Option 1. However, other measures reflect alternative approaches that are specific to each option and are not cumulative.

The policy measures have been designed to address the two identified problem areas in a complementary manner. Measures under Sub-policy Options 1.1, 2.1, 2.2 and 2.4 primarily address the persistent information gaps that hinder the development of a complete EU-wide criminal intelligence picture. Measures under Sub-policy Options 1.3, 1.4, 2.3 and 2.4 primarily address the fragmented and uneven use of Europol's operational support and specialised capabilities. Together, the measures seek to improve both the availability of operational information and Europol's ability to provide timely, effective and operationally embedded support to Member States and other relevant EU actors.

Policy Options (table):

	Policy Option 1: Reinforcing Europol's existing model	**Policy Option 2: Designing a new model for Europol**
Specific Objective 1: Reinforce Europol's role as an information hub for law enforcement		
a) closing information gaps	**Sub policy option 1.1**: strengthened data availability, processing and service	**Sub policy option 2.1**: Europol as an operational service provider and information hub for law enforcement
b) addressing data subject categorisation	**Sub policy option 1.2**: enhanced mitigating measures to address the obstacles of Data Subject Categorisation	**Sub policy option 2.2**: simplified rules to reduce the administrative burden of data subject categorisation
Specific Objective 2: Strengthening Europol's capacity to support law enforcement operational action		
a) inter-agency cooperation	**Sub policy option 1.3**: reinforced cooperation with the EU bodies and agencies for internal security	**Sub policy option 2.3**: Europol to provide analytical support to the EPPO
b) bringing Europol's support to the ground	**Sub policy option 1.4**: Europol digital platforms embedded in national investigations	**Sub policy option 2.4**: EU Digital Police Cloud and Europol support offices

4.1.1. Specific Objective 1: Reinforce Europol's role as the EU operational information hub for law enforcement

Policy Option 1: Reinforcing Europol's existing model

<u>Sub-policy option 1.1</u>: Strengthened data availability, processing and service

- Improving data availability through targeted and incremental data-sharing obligations
- Upgrading Europol systems and services to deliver stronger operational returns

This sub-policy option aims to strengthen Europol's ability to support Member State investigations by improving the **availability, timeliness and operational use of data**, while ensuring that enhanced cooperation delivers **clear operational returns** to Member States. It addresses the main technical, organisational and practical barriers to effective information exchange **without introducing automatic or bulk data transfers**, and without altering the fundamental data-ownership model or Europol's mandate.

The option focuses on **priority crime areas** identified in the Europol Regulation (e.g., terrorism and child sexual exploitation) where EU added value is clear. **Member States** would have **limited, progressive duties** to make relevant data available to Europol, building on existing cooperation practices.

A key measure is the **mandatory** deployment of technical **data-loader solutions**, enabling **automated and timely data uploads** while preserving **full Member State control** over shared data. Experience shows such tools reduce administrative burden, increase timeliness, and support more systematic information sharing. If all Member States were to contribute at levels comparable (per capita) to Member States equipped with data loaders (such as Germany and the Netherlands), the overall EIS content could potentially increase by 50% in the short term, providing a more comprehensive threat intelligence picture and a greater chance of identifying interconnected cases.

This approach does not alter the possibility left to Member States to decide not to supply information to Europol under Article 7(7) of the Europol Regulation, nor does it confer autonomous data collection powers on Europol. The focus is on **technical readiness, predictability and consistency**, supported by transparency measures such as monitoring of response times, feedback loops to national units and aggregated reporting on responsiveness.

A central component is a **major upgrade of Europol's ICT infrastructure and core systems** (including SIENA, EIS, EAS and QUEST/QUEST+)[101], improving scalability, automation, usability and performance. This ensures that increased data availability translates into tangible benefits for Member States. Where appropriate, proven EU technologies from EU large-scale systems provided by eu-LISA could be reused to

[101] See Annex 8 for more details.

enhance interoperability and resilience systems[102]. This increase in capacity would enable systematic and automated cross-check against relevant EU information systems[103].

Europol's role in maintaining **common technical and data standards**, notably the Universal Messaging Format (UMF), would be reinforced to reduce fragmentation, mapping costs and duplication, while supporting automation and data quality. The option also consolidates Europol's **OSINT capacity**[104], including the **application and deployment of AI-assisted tools**.

To reduce implementation costs, Europol could support **joint procurement of technical components** (e.g., data-loaders and interfaces), promoting economies of scale and interoperability. Crucially, the option strengthens Europol's **service and assistance role** through a dedicated pool of ICT and data-management experts supporting Member States with deployment, troubleshooting, standards compliance and training. This ensures consistent uptake and practical operational benefits.

Overall, this sub-policy option enhances the **availability, quality, and operational use of data** while fully respecting **national autonomy and data ownership**, functioning as both a standalone upgrade and a key enabler for broader reform measures.

Sub policy option 1.2: Mitigating measures to address the obstacles of Data Subject Categorisation

- Smarter and faster implementation of Data Subject Categorisation

This sub-policy option aims to **improve the efficiency** of DSC at Europol without changing the existing legal framework. It focuses on mitigating the resource-intensive nature of current requirements by strengthening Europol's operational procedures and technological capabilities.

In particular, Europol would deploy **advanced analytical tools** and update internal guidelines to support faster and more consistent DSC. This could include operational manuals and standardised procedures for handling specific datasets, such as telecommunications data, open-source intelligence or financial information. The objective would be to streamline the process, enhance legal certainty and reduce the operational burden. The option would also strengthen cooperation with Member States to facilitate the efficient processing of complex datasets and support timely investigations.

[102] For instance, technology used by the shared biometric matching service (sBMS) for upgrading Europol's biometric capabilities.

[103] In 2024, Europol carried out 13 704 manual and 194 792 batch searches directly in EIS and generated 13 409 Cross Match Reports and SIENA hit notifications. If each case-triggered intake (manual or batch) were systematically accompanied by proportionate consultations of relevant EU information systems (SIS, VIS, EURODAC, EES, ETIAS, ECRIS-TCN), this could imply in the order of 200 000 additional structured, logged queries annually at EU level.

[104] This would entail scaling up Europol's ability to collect and analyse publicly available online information relevant to criminal investigations. It would involve specialised tools, analytical methods and dedicated staff to systematically integrate OSINT into Europol's intelligence workflows.

Policy Option 2: Designing a new model for Europol

Sub policy option 2.1: Europol as an operational service provider and information hub for law enforcement

- Authorised Europol access to national data
- Europol as a provider of operational services

This sub policy option strengthens Europol's role as an **operational service provider acting on behalf of Member States**, by improving its ability to access, process and operationally exploit relevant information, while fully preserving **Member State data ownership, investigative autonomy and existing decentralised architectures**. It builds on existing EU frameworks, notably Prüm II[105], and focuses on targeted extensions where clear EU added value and operational necessity are demonstrated.

Under this option, Europol would be allowed, **with the explicit authorisation of the data-owning Member State(s)**, to query national databases already connected under EU information exchange mechanisms, in particular the Prüm II framework. This would include national biometric databases (DNA profiles, fingerprints and facial images), police record indexes (EPRIS) and vehicle registration data (EUCARIS).

The key change would be to **remove the current restriction linked to the origin of the data to be used by Europol** when launching queries, allowing Europol to use authorised national data in addition to third country-sourced data[106]. Europol would act strictly **on behalf of and within the scope defined by the authorising Member State(s)**[107].

For non-biometric data, this represents a proportionate extension of Europol's existing analytical role, removing an artificial constraint that limits operational effectiveness. For biometric data, Europol would function as a **technical and forensic service provider**, supporting Member States by launching authorised queries, handling complex matches and providing expert analysis, particularly in time-critical or large-scale cases (e.g., terrorist attacks or mass casualty events). Authorisations could be granted on a standing or ad-hoc basis.

Beyond data access, this option would also position **Europol as a provider of shared EU-level operational and technical services**, reducing fragmentation, dependencies, and costs. These services would be optional, demand-driven and subject to strong Member

[105] The Prüm II framework, established by Regulation (EU) 2024/982, is currently in the implementation phase, with the start of operations expected by 2027.

[106] Europol currently hosts roughly 17 600 fingerprints sets and 5 300 latent prints, around 450 DNA profiles, and about 3 500 facial images in the EIS. Extending the mandate to allow Europol to run Prüm II cross-checks not only on third-country biometrics but also on biometric data submitted by Member States would significantly enhance effectiveness. Instead of limiting queries to externally sourced datasets, Europol could systematically deconflict and crossmatch Member State-contributed biometric traces (e.g. latent prints from serious crime scenes) across the full Prüm network.

[107] This would not modify the Prüm II hit/no-hit architecture, nor grant Europol autonomous access rights.

State oversight. A key example is an **EU DNA matching service**[108], as Member States currently rely on different technologies, including third-country tools. An EU-level service facilitated by Europol would support **Prüm II implementation**, reduce external dependencies and ensure interoperability, while reducing dependency on third-country tools.

Sub policy option 2.2: Simplified rules to reduce the administrative burden of Data Subject Categorisation

- Aligning the rules with already existing legal frameworks

This sub-policy option would entail a legislative overhaul, aligning the Europol Regulation with the EU Data Protection Regulation (EUDPR) and the Law Enforcement Directive (LED), to establish an appropriate legal framework for Europol, simplifying the rules for data processing and improving Europol's operational flexibility, while maintaining a high level of data protection.

Under this approach, DSC would be required "where applicable and as far as possible", rather than as a strict *ex ante* condition for accepting and processing all data. Categorisation would instead take place when data is operationally used, allowing Europol to process larger and more complex datasets while ensuring proportionate and meaningful classification.

This framework would provide **greater legal clarity**, support the use of advanced analytical tools and machine learning by enabling more consistent processing and analysis of large and complex datasets, and reduce operational bottlenecks. Oversight by the European Data Protection Supervisor (EDPS) would remain. The alignment would also enhance consistency across EU data protection instruments, providing simplification and reducing fragmentation.

4.5.2. Specific objective 2: Reinforce Europol's role in providing operational support to investigations

Policy Option 1: Reinforcing Europol's existing model

Sub policy option 1.3: enhanced EU inter-agency information

- Reinforced operational support to the EPPO
- Strengthened Europol-Eurojust operational continuum
- Enhanced information sharing between Europol and AMLA

[108] DNA matching services are necessary tools to allow existing systems using DNA technology to work. Implementation would be progressive and evidence-based, starting with pilots and clear governance arrangements, preserving flexibility and trust. For more details on the EU DNA matching service, see Annex 9.

This option strengthens operational information exchange and cooperation between Europol and key EU bodies and agencies, notably the EPPO, Eurojust and AMLA, to ensure more coherent and effective EU-level support for national authorities in tackling cross-border crime.

Reinforced Europol support to the EPPO

This component would strengthen Europol's support to the EPPO while maintaining the current institutional framework. Europol would enhance its analytical support to EPPO investigations, ensuring more systematic and timely cooperation to be able to match the growing needs of the EPPO. This could involve allocating additional specialised staff within Europol, including the creation of a **dedicated team focusing on EPPO-related cases**. Such a team would deepen expertise, improve operational coordination and enable more structured planning of resources. The option would also strengthen operational interaction through enhanced coordination between liaison officers stationed at Europol and the EPPO.

These measures would require targeted legislative amendments but would not alter the respective mandates of Europol and the EPPO or the fundamental nature of their relationship.

Strengthened Europol-Eurojust operational continuum

This component would strengthen complementarity between Europol and Eurojust, ensuring a seamless continuum between law enforcement and judicial cooperation and enabling more integrated EU support throughout cross-border investigations. Operationally, this would support a more continuous transition between the intelligence, investigation and prosecution phases of cross-border cases, while avoiding duplication of efforts between authorities.

A first element of this measure would be to enhance information sharing by improving indirect access to information between Europol and Eurojust through the practical implementation of the **hit/no-hit system** provided for in the mandate of both agencies[109]. Under this system, each agency would be able to query limited reference data held by the other agency in order to identify whether potentially relevant operational or judicial information exists, without obtaining direct access to the underlying files. Operationally, this would involve upgrading the current mechanism through the implementation of more automated processes, thereby enabling faster and more efficient exchanges of relevant information between the two agencies.

A second element would establish **specialised EU-level support** within Europol for national authorities seeking to obtain electronic evidence from online service providers. This support would complement the judicial coordination role of Eurojust by focusing on the operational and technical dimensions of cross-border access to electronic evidence. This would include operational guidance on legal procedures, practical tools and technical expertise for requesting and handling electronic evidence, as well as structured channels for interaction with service providers. Europol's role would focus on facilitating operational coordination, technical assistance and information exchange, while judicial

[109] This solution would also be expanded to other EU bodies and agencies, ensuring a semi-automated and asymmetrical hit/no-hit system.

authorisations and prosecutorial decisions would remain the responsibility of competent national authorities and judicial actors. Europol could also maintain dedicated resources facilitating exchanges between competent authorities and providers, supporting the preservation, production and handling of electronic evidence in cross-border investigations. This would enable more consistent and predictable EU-level support in cases involving digital evidence and strengthen operational coordination between Europol and Eurojust.

Enhanced information sharing between Europol and the AMLA

This component would strengthen cooperation between Europol and the AMLA by enabling **structured information exchanges** between the two bodies. In particular, it would provide AMLA with indirect access to information stored by Europol through the hit/no-hit system. This would allow AMLA to identify potential links between financial intelligence and Europol's operational information on serious and organised crime.

Sub policy option 1.4: Embedding Europol tools and systems in national investigations

- Connect national case management systems
- Targeted obligation to consult Europol systems

This option would bring Europol's analytical capabilities closer to the daily work of investigators by integrating Europol tools directly into national case management systems. Instead of relying mainly on reactive exchanges of information, investigators would be able to access Europol's analytical support as part of their normal investigative workflow, allowing earlier identification of cross-border links and stronger analytical support throughout investigations.

Member States would progressively **connect their national case management systems** - to be established under Directive (EU) 2024/977 - with Europol systems through secure interfaces and common data standards. Investigators would be able to consult Europol systems automatically at predefined stages of an investigation, receive cross-checks and analytical feedback directly within their case files, and transmit relevant case information to Europol.

This approach would enable largely automated exchanges, allowing Europol to function as a shared analytical backbone by providing automated cross-checks and identification of cross-border connections in support of national investigations.

The option would also introduce a **targeted obligation to consult Europol systems** in serious and organised crime investigations with a cross-border dimension. Where relevant links are identified, this could trigger conditional sharing of case data with Europol, while fully respecting the principles of necessity and proportionality. Embedded consultation would support earlier detection of cross-border connections and help avoid investigative overlaps, complementing existing information exchange channels.

Implementation would depend on the development of fast, scalable and reliable digital infrastructure as envisaged under Sub policy option 1.1.

Policy Option 2: A new model for Europol

Sub policy option 2.3: Europol as structural provider of information, analytical support and capabilities to the EPPO[110]

- Integrated and systematic framework of operational and analytical support

This option would introduce a structural shift in Europol's support to the EPPO, moving from the current request-based model to a **systematic framework for analytical support**. Europol would act as a structural provider of analytical capabilities to the EPPO, ensuring that the Union's central law enforcement expertise is mobilised consistently in investigations affecting the Union's financial interests.

A key element would be the establishment of a structured framework through which Europol's analytical and technical capabilities are systematically deployed in support of EPPO investigations. This would include a **dedicated capability within Europol composed of specialised staff focusing on EPPO-related cases**, enabling deeper expertise and more predictable operational support.

Under this model, the EPPO would be able to **guide and prioritise the analytical support** provided by Europol, ensuring alignment with investigative needs and timelines and that analytical tasks and operational activities of a non-coercive nature are carried out by Europol **on behalf of the EPPO**. Europol would provide analytical support during operational phases of investigations, technical assistance in processing seized data, and intelligence products supporting investigative strategies. This would allow the EPPO to benefit more systematically from Europol's expertise in large-scale data analysis and criminal intelligence development in complex cross-border financial crime cases.

The option would also strengthen **information exchange** between Europol and the EPPO within the EPPO's mandate. The Europol Regulation could mirror the logic of the EPPO Regulation by allowing the EPPO to access relevant information held by Europol when this falls within its competence. Faster and more systematic data exchange would enable both bodies to identify cross-border criminal links more effectively and strengthen investigations affecting the Union's financial interests. Clear arrangements would govern the control and use of exchanged data, without fundamentally altering the existing data-ownership model or Europol's mandate.

Sub policy option 2.4: Operational integration of Europol into national investigations

- EU Police Cloud
- Europol Support Offices

[110] Policy Option 2 does not include a comparable operational support model for Eurojust, as the agency does not exercise investigative powers or conduct operational law enforcement activities.

This sub-option would transform the way Europol supports investigations by embedding its analytical, technical and coordination capabilities directly within national operational environments. Through a shared EU law enforcement platform ("EU Police Cloud") and reinforced operational presence in Member States, Europol would evolve from a central hub into an operational capability integrated into the day-to-day work of investigators across the Union.

EU Police Cloud

The EU Police Cloud would provide investigators in Member States with direct access to Europol's analytical tools, collaborative environments and data-processing capabilities through a secure digital platform. Rather than relying primarily on request-based support, investigators would be able to use Europol tools directly during investigations. Access would be granted only to authorised users designated by competent national authorities and Europol, based on role-based permissions and investigation-specific access rights. Authentication could rely on the EU Police Digital Identity, allowing national authorities to issue, manage and revoke credentials while ensuring a harmonised and trusted access framework across the Union.

The platform would remove technical barriers that currently limit the use of Europol's digital tools and progressively become accessible to a broad community of law enforcement users across the Union (up to 380 000 by 2035[111]). Designed as a modular online platform, it would allow investigators to access specialised tools and shared data in real time, enabling more timely and operationally embedded collaboration with Europol. In practice, investigators participating in the same join operational case could securely collaborate within dedicated digital workspaces, exchange operational information, perform analytical queries and coordinate investigative actions in near real time. The EU Police Cloud would bring together, through a **single digital environment**, the analytical and operational tools currently available at Europol's headquarters and make them accessible to national investigators across the Union.

A core function would be the ability to **upload, store and analyse large volumes of investigative data**, including structured data (police records, administrative data) and unstructured data (digital extractions, seized devices, operational material). Data uploaded to the platform would remain logically separated according to the relevant investigation, operational task or access authorisation. Data would remain subject to strict access control, compartmentalisation by investigation, and robust security safeguards, ensuring that only authorised personnel can access relevant datasets. All data-processing activities would be logged and auditable, enabling ex post verification of compliance with access rights, investigation mandates and data-protection requirements. Advanced forensic and analytical modules, including AI-based tools and biometric capabilities, would enable targeted cross-checks within joint investigations.

Other modules would **automate searches and requests** across information available for law enforcement purposes under Union or national law, including police records (EIS and national records via the Prüm II framework), investigative records, interoperability

[111] Estimation based on the assumption that (i) 20% of law enforcement officers have criminal investigation skills, and (ii) the size of the European police workforce reported by Eurostat (2023): 1,537,588 police officers. Police, court and prison personnel statistics - Statistics Explained - Eurostat.

databases, national administrative records (see policy option 1.1), OSINT, referrals, information provided by third countries or private parties to Europol. Queries would be taking place in accordance with applicable access rights and legal bases, ensuring that users only obtain access to information they are authorised to consult. To improve reactivity, regular repeated searches and **alerts** would be implemented.

As collaboration builds upon a continuum of exchanges from the more technical to the more communicational, this platform would provide online integrated collaboration tools building on existing Europol tools[112] such as messaging, mail and video conference. These functionalities would support operational coordination between investigators and analysts.

To handle increasing data, processing and users, the platform would use **multi-cloud infrastructure** (private and sovereign), allowing differentiated treatment of sensitive areas like terrorism. Sensitive operational environments could be hosted within dedicated secured infrastructures with reinforced access restrictions and cybersecurity measures. It would be accessible as a **standalone web/mobile application** and via Application Programming Interfaces (APIs)[113] for integration with national case management systems, supporting Europol's standardisation role. Security would rely on a **harmonised EU Police Digital Identity** based on the EU Digital Identity Framework at high assurance level granting secure and trusted access across the Union. The platform would be developed according to security-by-design and security-by-default principles. Cybersecurity safeguards would include multi-factor authentication, encryption, continuous security monitoring, incident detection and response capabilities, audit trails and resilience measures against unauthorised access, data breaches or cyberattacks. Sensitive operational environments could be subject to enhanced security requirements depending on the nature of the data processed. Successful implementation would depend on the simplification of the DSC under Sub policy option 2.2 to allow for Europol to process data even if the DSC has not yet been carried out.

Europol support offices

Europol support offices would strengthen Europol's operational presence in Member States and **serve as interfaces with national authorities**, helping investigators integrate Europol's tools, analysis and expertise into ongoing investigations. They could build on the existing Europol National Units in each Member State.

The model would rely on staffing arrangements that combine expertise on Europol and its tools with strong familiarity with national investigative environments. This would allow Europol's support to be better aligned with national legal frameworks, procedural requirements and investigative workflows.

Through this approach, Europol support offices would act as operational multipliers within national investigative ecosystems. They would provide investigators with immediate operational access to Europol's analytical tools, specialist expertise and technical capabilities, enhancing awareness of Europol's support and effectively embedding that support within investigations. By enabling the early mobilisation of Europol capabilities,

[112] Including SIENA, Videoconference for Operational Purposes (VCOP) and Virtual Command Post (VCP).
[113] APIs are sets of rules and protocols that allows different software applications or systems to communicate and exchange data with each other.

they would ensure that analytical outputs and technical support are produced in forms that can be **directly integrated into national investigative processes** and, where relevant, relied upon in judicial proceedings.

The support offices would also provide a **stable operational interface** for the deployment of specialised Europol capabilities, including digital forensic expertise, data analysis and other technical support. This model would complement the Agency's strong central model while bringing Europol's capabilities closer to investigators on the ground. It would also support a more circular exchange of expertise between Europol and national authorities, strengthening operational cooperation and the practical use of Europol capabilities across the Union.

5.3. Options discarded at an early stage

5.3.1.
Non-legislative action and targeted changes to Europol's legal framework

Non-legislative measures, including operational arrangements, guidance, and technical improvements within the existing legal framework, were considered but found insufficient to address the structural limitations identified. While such measures could deliver incremental improvements, they would not enable Europol to access, process, and operationally exploit information at the scale required, nor to strengthen its operational support, capabilities, and governance in a systematic and sustainable manner.

Similarly, more limited and isolated amendments to the Europol Regulation were considered but discarded, as they would not provide the comprehensive and future-proof framework needed to enable Europol to operate effectively in a rapidly evolving and increasingly complex security environment[114]. Targeted legislative adjustments may address specific issues, but, on their own, would not fully address the broader structural challenges identified.

5.3.2.
Turning Europol into an autonomous agency with executive powers

The option of transforming Europol into an autonomous agency with executive law enforcement powers, including the ability to conduct investigations or take coercive measures independently of Member State authorities, was considered[115] but discarded at an early stage. Such an approach would represent a fundamental departure from the current role of Europol as a support and coordination agency operating in close cooperation with national authorities in line with Article 88 TFEU.

---

[114] The Commission's report pursuant to Article 68(3) of the Europol Regulation (COM(2025) 752 final) illustrates that limited changes risk to perpetuate existing shortcomings.

[115] Some stakeholders, including the European People's Party and Renew Europe, have called for strengthening Europol's operational role, including proposals to grant enforcement powers. https://www.epp.eu/files/uploads/2025/01/EPP-Retreat-Priorities-2025-statement.pdf

This option would raise significant legal, operational and governance complexities. Consequently, this option will not be available in short- to mid-term to address the pressing security needs identified in Section 2.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This section assesses the expected impacts of the policy options described in Section 5. The analysis evaluates the extent to which the options would contribute to achieving the objectives identified in Section 4, compared with the baseline scenario described in Section 5.3. The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'neutral' (0) and 'negative impact' (-).

The assessment draws on the evidence collected through the study supporting this Impact Assessment, including, where possible, the quantification and monetisation of impacts. Where sufficient data was available, impacts were quantified based on existing assessments or modelling; where this was not possible, a qualitative assessment was carried out. Further details on the methodology and underlying estimates are provided in Annex 10.

6.1 Financial impacts[116]

Impact on EU institutions and agencies

Policy Option 1 (+/-) entails additional financial and human resource requirements for Europol. Over the 2028–2034 Multiannual Financial Framework (MFF) period, **one-off adjustment costs** are estimated at approximately **EUR 61 million**[117], mainly associated with upgrades of ICT infrastructure including the EIS, the EAS, SIENA, QUEST and analytical tools supporting operational information exchange and analysis. Europol would also incur **recurring annual adjustment costs of around EUR 12.2 million**[118] (corresponding to approximately EUR 85.4 million cumulatively over the 2028–2034 period) related to staff, system maintenance, infrastructure operation and technical support to Member States[119].

Additional costs related to mitigating measures on DSC are expected to remain limited, as they mainly concern the development of internal guidance, analytical tools and training materials[120].

Policy Option 1 also includes measures reinforcing operational cooperation between Europol and other EU bodies and agencies. In particular, strengthening Europol's support to the EPPO would require the establishment of a dedicated analytical and operational support capacity within Europol. The recurring annual operational cost of this reinforced

[116] Detailed information is provided in Annex 3.
[117] See costs section of Annex 3.
[118] See costs section of Annex 3.
[119] These costs relate mainly to the upgrade and scaling of Europol's core systems and the provision of technical support to Member States. These costs include the staff needed to provide the services.
[120] Costs mainly concern the development of internal operational guidance, analytical tools and training activities aimed at improving the efficiency of data subject categorisation processes.

support is estimated at approximately **EUR 10 million**[121] (corresponding to approximately EUR 70 million cumulatively over the 2028–2034 period). Furthermore, measures strengthening the operational continuum between Europol and Eurojust would generate **limited additional EU-level financial costs**, estimated at approximately **EUR 2 million in one-off costs and EUR 1 million in recurring annual adjustment cost** (corresponding to approximately EUR 7 million cumulatively over the 2028–2034 period), mainly related to system adaptations and operational coordination[122].

Finally, the integration of Europol analytical tools and systems into national investigative environments would require additional investment at Europol level, with **one-off adjustment costs estimated at approximately EUR 50 million and recurring annual adjustment cost of around EUR 8 million**[123] (corresponding to approximately EUR 56 million cumulatively over the 2028–2034 period).

Under **Policy Option 2**, the financial impact on EU institutions and agencies would be more significant **(+).**

For Europol, one-off adjustment costs are estimated at approximately **EUR 11 million**, mainly linked to system adaptations, reinforced data-management capacity and the development of an EU DNA matching service. Europol would also incur **recurring annual adjustment cost of around EUR 5.3 million** (corresponding to approximately EUR 37.1 million cumulatively over the 2028–2034 period), primarily related to specialised staff, system maintenance and operational support associated with these services[124]. However, these investments could generate efficiency gains at EU level by reducing fragmentation, avoiding duplication of technical solutions across Member States and providing shared operational services at scale.

Furthermore, additional financial effects would arise from the **simplification of the rules on DSC**. While this policy option would significantly improve Europol's operational flexibility and capacity to process information, it would not require substantial financial investment, as it mainly involves legislative alignment and simplification of existing rules. On the contrary, the simplification of the current framework is expected to generate **administrative savings and efficiency gains**, as resources currently devoted to the labour-intensive process of DSC could be redeployed to operational analysis and investigative support. Overall, the measure is therefore expected to have a **very positive financial impact**, primarily through efficiency gains rather than additional expenditure, although these gains remain difficult to quantify precisely at this stage due to limited comparable operational data.

---

[121] Costs relate primarily to specialised staff within a dedicated Europol support capacity responsible for operational analysis, cross-checks of operational data and digital forensic support for EPPO investigations. 52 additional officers would be required in 2026, gradually increasing to 66 officers by 2033, to meet the growing demand for support. The total annual cost of employing these additional officers is estimated to rise from €8.2 million in 2026 to €10.4 million by 2033.

[122] These costs relate to further development of the Europol-Eurojust hit/no-hit information exchange mechanism and the consolidation of EU-level support for accessing electronic evidence.

[123] See costs section of Annex 3.

[124] Costs relate mainly to system adaptations enabling authorised access to national databases connected under EU frameworks, reinforced data management capacity and the development and operation of an EU DNA matching capability.

The development of the **EU Police Cloud** would entail **one-off adjustment costs for Europol estimated at approximately EUR 143.3 million** and **recurring annual adjustment cost of around EUR 39.8 million**[125] (corresponding to approximately EUR 278.6 million cumulatively over the 2028–2034 period). While the initial investment in digital infrastructure is significant, the use of a common EU-level platform is expected to generate efficiency gains over time by reducing fragmentation between national systems and enabling more efficient processing and analysis of operational data[126].

Additional costs would arise from the **deployment of Europol support offices in Member States**, with **recurring annual adjustment cost of up to EUR 6.5 million**[127] (corresponding to approximately EUR 45.5 million cumulatively over the 2028–2034 period).

Establishing Europol as a structural provider of analytical and operational support to the EPPO would generate **additional adjustment recurring cost at EU level estimated at approximately EUR 11 million per year**[128] (corresponding to approximately EUR 77 million cumulatively over the 2028–2034 period). These costs relate mainly to the creation and operation of a dedicated Europol support capacity composed of specialised analysts and operational staff supporting EPPO investigations[129]. No separate one-off adjustment costs are expected[130].

Impact on Member States

Under **Policy Option 1 (+),** Member States would incur **moderate implementation costs**, mainly related to improving data exchange with Europol and integrating Europol analytical capabilities into national investigative environments.

One-off costs are estimated at approximately **EUR 81 million in total (around EUR 3 million per Member State on average)**, primarily linked to the deployment of automated data-loader solutions and the technical adjustments required to connect national systems with upgraded Europol platforms. Recurring annual costs are estimated at approximately **EUR 16.2 million** (corresponding to approximately EUR 113.4 million cumulatively over the 2028–2034 period), mainly related to maintenance of data loader infrastructure, system interfaces and operational support.

Further costs would arise from the **integration of EIS and EAS into national investigative environments**, including updates to national case management systems, the adoption of common data standards and training of personnel. These investments are estimated at approximately **EUR 105 million in one-off costs and EUR 20 million in**

[125] Costs relate mainly to infrastructure development, system integration, data migration and the operation of the EU Police Cloud platform, as well as the establishment of a secure EU Police Digital Identity framework for law enforcement users.
[126] See benefits section of Annex 3.
[127] See costs section of Annex 3.
[128] See costs section of Annex 3.
[129] Costs primarily reflect the establishment of a dedicated EPPO support team within Europol responsible for operational analysis, cross-checks of operational data, digital forensic support and coordination of analytical activities supporting EPPO investigations.
[130] The necessary infrastructure and onboarding requirements are already covered.

annual recurring costs (corresponding to approximately EUR 140 million cumulatively over the 2028–2034 period).

At the same time, Policy Option 1 is expected to generate **significant operational efficiencies for national authorities**[131]. Automated data loaders would reduce manual processing and delays in information sharing, while improved Europol systems and embedded analytical services would allow investigators to benefit more systematically from EU-level analytical capabilities. Measures addressing obstacles linked to DSC would **not generate additional costs for Member States**, as they mainly concern internal procedures within Europol.

Under **Policy Option 2 (+/-),** the economic impact on Member States would vary depending on the operational capabilities developed at EU level.

For measures enabling Europol to act as an **operational service provider and information hub**, Member State costs are expected to remain **very limited**, as the approach relies primarily on existing EU information exchange mechanisms, such as the Prüm II framework. One-off costs are estimated at approximately **EUR 0.05 million per Member State**[132], reflecting minor technical adjustments required to enable authorised queries through existing infrastructure. Recurring costs are expected to remain negligible.

More substantial costs would arise from the **deployment of the EU Police Cloud and related digital infrastructure**, which would require adjustments to national systems, integration with the EU Police Digital ID framework, training and data migration. These investments are estimated at approximately **EUR 67.5 million in one-off costs and EUR 11.4 million in annual recurring costs**[133] (corresponding to approximately EUR 79.8 million cumulatively over the 2028–2034 period).

Overall, although Policy Option 2 involves high implementation costs for Member States in relation to digital infrastructure, these investments are expected to generate **long-term efficiency gains** by enabling access to shared analytical tools and operational services at EU level, reducing fragmentation of national solutions and supporting more effective cross-border investigations.

6.2 Social impacts

6.2.1 Impacts on security and EU citizens

Policy Option 1 (+) is expected to have a positive impact on internal security by strengthening the ability of national authorities and EU bodies to detect and investigate cross-border criminal activity. Improved data availability and upgraded Europol systems would enable more systematic cross-checks and faster analytical support, helping investigators identify cross-border links earlier and coordinate more effectively.

Reinforced cooperation with the EPPO would reinforce investigations affecting the Union's financial interests, while stronger coordination with Eurojust would facilitate the

[131] See benefits section of Annex 3.
[132] See costs section of Annex 3
[133] See costs section of Annex 3

judicial handling of complex cross-border cases, including those involving electronic evidence. Embedding Europol analytical tools within national investigative workflows would further reduce the risk of undetected cross-border criminal connections, ultimately contributing to a higher level of security for EU citizens.

Policy Option 2 (++) is expected to have a very strong positive impact on security by significantly strengthening the Union's ability to detect, investigate and disrupt serious and organised crime. Faster and more systematic cross-checks across national databases under the Prüm II framework would enable investigators to identify cross-border criminal networks earlier and act more quickly. Shared EU-level operational capabilities and simplified data processing rules would substantially increase Europol's analytical capacity, allowing authorities to exploit large datasets and detect criminal patterns that would otherwise remain unnoticed.

By making Europol's capabilities directly accessible to investigators through shared digital infrastructure and strengthened operational presence in Member States, the option would enable faster, more coordinated and intelligence-driven investigations across the Union. Overall, this option would markedly improve the EU's ability to prevent and disrupt cross-border crime and terrorism, delivering tangible security benefits for EU citizens.

6.2.2 Administrative impacts on national authorities

Policy Option 1 (+) is expected to have a positive impact on the administrative efficiency of national law enforcement authorities by streamlining cross-border information exchange and improving the operational returns of cooperation with Europol. Improved data availability and automated data-sharing tools would reduce manual administrative tasks and delays, while upgraded Europol systems would provide faster cross-checks and analytical support. Additional efficiency gains would arise from clearer guidance on DSC and strengthened cooperation with EU bodies and agencies. Embedding Europol tools more directly into national investigative workflows would further reduce administrative friction and improve the systematic use of EU-level information in investigations.

Policy Option 2 (++) would result in strong administrative efficiency gains by simplifying procedures and expanding EU-level operational support. Allowing Europol, when authorised by Member States, to query national databases under the Prüm II framework would reduce administrative workload in cross-border investigations and enable Europol to carry out complex analytical and forensic tasks on behalf of Member States. Further gains would arise from establishing Europol as a structural provider of analytical support to the EPPO to avoid multiple requests for information. The EU Police Cloud and Europol support offices would also facilitate easier access to Europol tools and expertise, improving operational interaction and reducing coordination burdens for national authorities.

6.2.3 Youth impacts

Both policy options (0) are not expected to have direct impacts specifically targeting young people. However, by strengthening the Union's capacity to prevent and combat serious and organised crime, including offences that particularly affect minors, such as child sexual

exploitation or cyber-enabled crime, the measures may have indirect positive effects on young people.

6.2.4 SMEs

Both policy options concern the operational framework, governance and cooperation mechanisms of Europol and competent public authorities. It does not introduce regulatory obligations, compliance requirements or direct operational impacts for SMEs. Both policy options are therefore not expected to have direct impacts for SMEs.

6.3 Fundamental rights impacts

The two policy options assessed in this Impact Assessment involve the processing of personal data in the context of law enforcement cooperation. They therefore relate primarily to the fundamental rights to **respect for private and family life (Article 7)** and **protection of personal data (Article 8)** of the Charter of Fundamental Rights of the European Union. The analysis below assesses whether any interference with these rights is necessary and proportionate to the objective of general interest consisting in the prevention, detection and investigation of serious and organised crime and terrorism.

6.3.1 Objective of general interest

Policy Option 1 (++)

Policy Option 1 contributes to the objective of general interest consisting in the prevention, detection and investigation of serious and organised crime and terrorism. By improving the availability, quality and timeliness of operational data exchanged between Member States and Europol, the option would strengthen the analytical capacity of law enforcement authorities and support earlier identification of cross-border criminal links. Upgrading Europol's systems and improving data exchange with other EU bodies and agencies would allow authorities to exploit operational information more effectively.

Policy Option 2 (++)

Objective of general interest

Policy Option 2 would further strengthen the Union's capacity to prevent, detect and investigate serious and organised crime and terrorism by significantly improving the ability of law enforcement authorities to access, process and analyse operational data across borders. By enabling faster cross-checks across databases, expanding EU-level analytical capabilities and simplifying data processing rules, the option would allow authorities to exploit large and complex datasets more effectively in support of investigations. This would enhance the detection of criminal networks, strengthen cross-border investigations and improve the overall effectiveness of EU action against serious and organised crime.

6.3.2 Protection of personal data

Policy Option 1 (0)

Necessity

The measures included in Policy Option 1 aim to address operational inefficiencies in the current framework for information exchange and analysis. In particular, fragmented and

largely manual data-sharing processes limit the ability of Europol and Member States to analyse operational information effectively and identify cross-border criminal connections. Improving data availability through automated tools and upgrading Europol systems would ensure that lawfully shareable information can be processed more efficiently and used more systematically in criminal investigations.

At the same time, the option does not introduce new categories of personal data, new processing purposes, or additional access rights. The measures primarily concern improvements to the functioning of existing systems and procedures and therefore operate within the current legal framework governing the processing of personal data by Europol and national authorities.

While the option does not substantially alter the existing data-protection framework, increased automation and interoperability may nevertheless increase certain risks related to erroneous data propagation, unauthorised access or wider dissemination of inaccurate information if safeguards are not effectively implemented.

Proportionality

The option preserves the existing safeguards governing the processing of personal data. Member States would retain control over the data they share with Europol and existing rules on purpose limitation, access conditions and retention periods would remain unchanged. Measures addressing operational challenges related to data subject categorisation would focus on improving procedures and guidance rather than modifying the underlying legal obligations.

Operational safeguards would continue to include role-based access controls, logging and traceability of access to operational data, differentiated handling codes defined by the data owner, data-quality verification mechanisms, and supervision by the Europol Data Protection Officer and the European Data Protection Supervisor (EDPS). Europol's existing information-security framework, including encryption, network segmentation, secure authentication mechanisms and continuous security monitoring, would continue to apply to upgraded systems and automated exchange tools.

In practice, automated data-loading solutions would not bypass Member State control over operational data. Member States would remain responsible for defining which categories of information may be shared automatically, under which conditions, and with which handling restrictions. Automated exchanges would therefore remain subject to predefined operational parameters, auditability and ex post verification mechanisms.

Conclusion

Overall, Policy Option 1 respects the principles of necessity and proportionality while maintaining the existing level of data protection safeguards. Its impact on the protection of personal data is therefore assessed as **neutral (0)**. Although certain operational risks linked to increased automation remain, these are considered limited and manageable within the existing EU data protection, cybersecurity and supervisory framework.

Policy Option 2 (-)

Necessity

The measures address operational limitations currently affecting cross-border investigations, particularly delays and fragmentation in accessing and analysing operational data. Allowing Europol, when authorised by Member States, to perform queries in national databases connected under existing EU frameworks would enable faster identification of cross-border links in complex or time-critical investigations. Shared services, such as a potential EU DNA matching service, would strengthen forensic cooperation and reduce reliance on fragmented technical solutions.

In addition, the EU Police Cloud would provide the scalable infrastructure required to process large and complex datasets used in cross-border investigations, while the simplification of DSC rules would allow lawfully collected data to be processed more efficiently. These measures are therefore necessary to ensure that operational information can be effectively used to combat increasingly digital and transnational forms of crime.

At the same time, these measures increase the scale, speed and interconnectedness of operational data processing, thereby creating heightened risks relating to cybersecurity, unlawful access, function creep, excessive data availability, potential re-use of data beyond the original operational context, and the processing of inaccurate or insufficiently categorised data. The EU Police Cloud in particular would create a more integrated operational environment with a significantly larger user base and increased volumes of sensitive law-enforcement information processed digitally across borders.

Proportionality

The interference with fundamental rights remains proportionate. Europol would act only on the basis of Member State authorisation and within its mandate, without centralising national databases or altering Member State ownership of data. The measures do not introduce fundamentally new categories of personal data or new processing purposes but improve the operational use of data already lawfully collected for law enforcement purposes.

Processing would remain subject to the safeguards provided under the Europol Regulation, the Law Enforcement Directive and the EUDPR, including purpose limitation, access controls and independent supervision. Technical infrastructures such as the EU Police Cloud would incorporate security-by-design features, strong authentication and traceable access management to ensure accountability.

More specifically, the EU Police Cloud would rely on a multi-layered security architecture combining organisational, technical and legal safeguards. These would include end-to-end encryption of data in transit and at rest, strict compartmentalisation of operational datasets, role-based and attribute-based access controls, multi-factor authentication through the EU Police Digital Identity framework, continuous security monitoring, penetration testing and detailed audit logs enabling full traceability of user actions.

Access to operational environments and datasets would remain limited to specifically authorised users acting within defined operational mandates and on a need-to-know basis. Different investigations and operational projects would remain logically separated through compartmentalised access environments, preventing unrestricted cross-access to operational information.

The processing of sensitive operational datasets would also remain subject to differentiated handling codes, retention periods and supervisory controls. Europol's Data Protection

Function and the EDPS would continue exercising oversight over compliance with data-protection obligations, including in relation to large datasets, automated analytical tools and the use of artificial intelligence-supported functionalities.

Regarding the simplification of DSC rules, safeguards would continue to require Europol to assess the relevance, reliability and necessity of operational data within defined timeframes. The simplification would therefore not eliminate data-protection obligations, but rather adapt the sequencing and operational handling of categorisation requirements to avoid unnecessary delays in time-sensitive investigations, therefore aligning it with the EUDPR.

Cybersecurity risks associated with the EU Police Cloud would furthermore be mitigated through compliance with the EU cybersecurity framework applicable to Union institutions and bodies, including high common cybersecurity standards, incident reporting obligations, business continuity measures, security accreditation procedures and continuous vulnerability management. Given the sensitivity of the data processed, implementation would likely require phased deployment, independent security testing and reinforced operational-security governance arrangements.

Conclusion

Overall, Policy Option 2 would increase the operational processing of personal data within EU law enforcement cooperation and therefore has a **negative impact (-) on the protection of personal data** compared with the baseline. Nevertheless, the interference with fundamental rights remains **justified by the objective of combating serious and organised crime and terrorism**, and the measures are **necessary and proportionate**, while maintaining the safeguards and oversight mechanisms provided by the EU data protection framework.

Although residual risks related to cybersecurity, data concentration and broader operational access cannot be fully eliminated, these risks are expected to be mitigated through a combination of legal limitations, technical safeguards, operational controls and independent supervision. The overall impact on fundamental rights is therefore considered proportionate in light of the security objectives pursued and the safeguards accompanying implementation.

6.4 Environmental impacts

Both policy options are not expected to have direct environmental impacts (0), as they concern the organisation of law enforcement cooperation and the analytical and operational support provided by Europol. However, the options could have indirect positive effects on the environment. Environmental crime is included among the areas of criminal activity listed in Annex I of the Europol Regulation. By strengthening Europol's analytical capabilities, operational support and cooperation with national authorities, **Policy Options 1 and 2 could contribute to more effective detection and investigation of environmental crime**, such as illegal waste trafficking or wildlife trafficking.

7 HOW DO THE OPTIONS COMPARE?

This section compares the policy options presented in Section 5 against the baseline scenario described in Section 5.3 and assesses their relative effectiveness in achieving the objectives identified in Section 4.

Overall, both policy options would improve Europol's capacity to support Member States in preventing and combating serious and organised crime and terrorism. However, they differ in the scale of change introduced, the level of investment required and the extent to which Europol's operational role within the EU internal security architecture would evolve. **Policy Option 1 focuses on reinforcing and modernising the existing cooperation model, whereas Policy Option 2 introduces a more integrated operational model with stronger EU-level capabilities.**

7.1. Addressing information gaps

Both policy options address **two closely linked aspects of the problem**: the availability of operational information shared with Europol and the conditions under which Europol can process and that information.

Policy Option 1 (Sub policy options 1.1 and 1.2) focuses on improving the functioning of the existing information exchange model, notably through automated data loaders, targeted data-sharing obligations and upgrades to Europol's core information systems.

In terms of effectiveness, these measures would significantly improve the availability, quality and timeliness of operational information available to Europol, thereby strengthening its analytical support to Member States. However, the option would not fully address structural constraints affecting Europol's capacity to process large and complex datasets, as the current framework for data subject categorisation would remain unchanged. At the same time, information sharing would continue to rely largely on voluntary contributions by Member States.

In terms of efficiency, the option requires investment in digital infrastructure and system upgrades but largely builds on existing systems and cooperation mechanisms. These investments are expected to generate operational efficiencies through improved automation and interoperability.

Regarding coherence, the option fully preserves the current decentralised model of information exchange and maintains Member States' control over operational data.

In terms of fundamental rights, the option improves data-sharing efficiency within existing safeguards and does not introduce new data, purposes or access rights.

Policy Option 2 (Sub policy options 2.1 and 2.2) introduces an integrated model by allowing Europol, where authorised by Member States, to query certain national databases connected under EU frameworks and by simplifying the rules governing the processing of operational data by reforming data subject categorisation.

In terms of effectiveness, these measures would significantly improve Europol's ability to identify cross-border links and process large operational datasets, thereby enabling more systematic use of advanced analytical tools.

In terms of efficiency, the option involves higher implementation costs, particularly related to the development of shared operational capabilities and digital infrastructure.

However, it may also generate long-term efficiency gains by reducing fragmentation of analytical tools across the Union.

Regarding coherence, the option represents a more significant evolution of Europol's operational role, but remains compatible with the EU legal framework, as Europol would continue to act in support of Member States.

In terms of fundamental rights, the option would increase the operational processing of personal data compared with the baseline. Such processing would nevertheless remain subject to the safeguards and oversight mechanisms provided under EU data protection law.

Criterion	Baseline	Policy option 1	Policy option 2
Effectiveness	0	+	++
Efficiency	0	+	+
Coherence	0	+	+
Fundamental rights	0	0	-

7.2. Addressing operational gaps

Both policy options addressing this problem concern Europol's capacity to provide operational support to investigations across the Union. These limitations relate both to the level of operational support provided to Member States and to the coordination of EU-level support between Europol and other EU actors involved in combatting cross-border crime.

Policy Option 1 (Sub policy options 1.3 and 1.4) focuses on reinforcing the existing operational cooperation model by strengthening coordination between Europol and other EU actors and by bringing Europol's capabilities closer to national investigators.

In terms of effectiveness, these measures would improve the overall EU support architecture for cross-border investigations. Embedding Europol tools into national investigative workflows would support earlier identification of cross-border links and allow Europol's analytical capabilities to be used more systematically by national authorities. Strengthened cooperation between Europol, the EPPO and Eurojust would also facilitate more efficient handling of complex cases. However, the option would primarily reinforce the current cooperation model and would not fundamentally transform how Europol's capabilities are accessed and used by investigators.

In terms of efficiency, the option requires significant investment in system integration and digital infrastructure, particularly to embed Europol analytical tools into national case management systems. At the same time, these investments build on existing cooperation structures and are expected to generate operational efficiencies by reducing administrative

burdens associated with manual information exchange and by improving the timeliness of analytical support.

Regarding coherence, the option preserves the existing institutional balance within the EU internal security architecture. Europol would continue to operate as a support agency acting in close cooperation with national authorities and other EU actors.

Policy Option 2 (Sub policy options 2.3 and 2.4) introduces a more integrated operational model aimed at bringing Europol's capabilities closer to investigators and strengthening its role as a provider of operational services at EU level.

In terms of effectiveness, these measures would significantly enhance Europol's operational support to investigations. The EU Police Cloud and Europol support offices would enable investigators to access Europol's analytical tools, collaborative environments and technical capabilities more directly during investigations, facilitating large-scale collaborative investigations and more effective use of advanced analytical tools. At the same time, establishing Europol as a structural provider of analytical capabilities to the EPPO would ensure a more systematic use of Europol's expertise in complex cross-border cases.

In terms of efficiency, the option involves substantial investment in digital infrastructure and operational capacity, particularly for the development of the EU Police Cloud and the deployment of support offices in Member States. However, the use of shared EU-level analytical tools and collaborative environments could generate long-term efficiency gains by reducing fragmentation of national solutions and enabling more efficient cross-border investigations.

Regarding coherence, the option represents a more significant evolution of Europol's operational role within the EU internal security architecture. The measures would remain compatible with the existing institutional framework for EU law enforcement cooperation.

In terms of fundamental rights, the option could lead to a moderate increase in the operational processing of personal data compared with the baseline, notably due to the more systematic and collaborative use of Europol's analytical tools within the EU Police Cloud. In addition, the simplification of the DSC framework would expand the categories of personal data that Europol may process for operational analysis in certain cases, where the DSC is not immediately possible and must be carried out *as far as feasible and as early as possible*. This may increase the volume of personal data processed compared with the baseline. At the same time, the use of a common EU-level infrastructure could also strengthen safeguards by enabling more consistent security standards, access controls and audit mechanisms across the Union. In any event, such processing would remain subject to the safeguards and oversight mechanisms provided under EU data protection law.

Criterion	Baseline	Policy option 1	Policy option 2
Effectiveness	0	+	++

Efficiency	0	+	+
Coherence	0	+	+
Fundamental rights	0	0	-

8 PREFERRED OPTION

Based on the comparison of policy options in Section 7 and the impacts assessed in Section 6, the preferred approach consists of a package of measures **combining elements** from Policy Options 1 and 2. This approach addresses both the information gaps affecting Europol's role as an information hub and the operational limitations that constrain timely and effective support to investigations, with advanced capabilities acting as a cross-cutting enabler.

Specific objective	Policy option	Main measure
Information exchange	Policy Option 1 (Sub policy option 1.1)	Strengthened data availability, processing and service
Information exchange and advanced capabilities	Policy Option 2 (Sub policy option 2.1)	Extension of Europol access to relevant data via the Prüm II framework
Information exchange	Policy Option 2 (Sub policy option 2.2)	Reform of Data Subject Categorisation
Operational support	Policy Option 1 (Sub policy option 1.3)	Enhanced EU inter-agency cooperation with Eurojust, AMLA
Operational support	Policy Option 2 (Sub policy option 2.3)	Structural Europol-EPPO partnership
Operational support	Policy Option 1 (Sub policy option 1.4)	Embedding Europol tools and systems in national investigations
Operational support and advanced capabilities	Policy Option 2 (Sub policy option 2.4)	Operational integration of Europol into national investigations (EU Cloud, Europol support offices)

Taken together, these measures form a **coherent and mutually reinforcing reform** of the EU law enforcement information architecture.

Options not retained

Several elements considered during the assessment were not retained in the preferred package. In particular, **Sub policy option 1.2 was not retained**, as the targeted improvements in data availability and automation provided under Sub policy options 1.1, 1.4 and 2.4, **combined with the structural reform of data subject categorisation introduced under Sub policy option 2.2**, provide a more effective and coherent framework for operational data processing. At the same, **Sub policy option 1.3** is also not retained because exploiting the full potential between Europol and the EPPO requires substantial reinforcements.

8.1. Impacts of the preferred option

Cumulative impact of the preferred package

The preferred package generates cumulative impacts by combining measures that address **different but interrelated drivers of the problem**. Taken together, these measures strengthen Europol's ability to combat cross-border crime more effectively than any individual measure alone.

First, improvements in data availability and usability (Sub policy options 1.1, 2.1, 2.2 and 1.4) enhance Europol's capacity to receive, process and analyse operational information. This **strengthens the analytical basis for cross-border investigations** and improves the quality and timeliness of criminal intelligence products provided to Member States.

Second, reinforced cooperation with EU actors, notably Eurojust and the EPPO (Sub policy options 1.3 and 2.3), improves **the coordination between operational and prosecutorial support at EU level**. This facilitates more effective follow-up of operational criminal intelligence and strengthens the overall EU response to serious and organised crime.

Finally, the EU Police Cloud and related operational integration measures, including Europol support offices (Sub policy option 2.4), provide the **scalable digital and operational infrastructure** needed to support more advanced data analysis and closer day-to-day operational cooperation between Europol and national authorities, including in support of ongoing investigations.

By combining these elements, the preferred package improves the flow of information, strengthens operational coordination and provides the technical capabilities needed to support more integrated EU law enforcement cooperation.

8.1.1 Financial impacts (+)

The preferred package entails cumulative investments at both Member State and EU level while generating important efficiencies through synergies between the selected measures.

In particular, overlaps between Sub policy options 1.1 and 1.4 generate **economies of scale.** As some infrastructure and implementation costs are shared, the combined implementation reduces costs by an estimated **EUR 30 million** in one-off expenditure and **EUR 6 million in recurring annual costs** (corresponding to approximately EUR 42

million over the 2028–2034 MFF period) compared with a scenario where the options would be implemented separately.

The total estimated costs[134] are:

Costs	Member States	Europol
One-off costs	EUR 254.85 million	EUR 239.8 million
Annual recurring costs	EUR 47.9 million	EUR 78.4 million
Recurring costs cumulative 2028-2034	EUR 335.3 million	EUR 548.8 million
Total costs over 2028–2034 (one-off + recurring)	EUR 590.15 million	EUR 788.6 million

8.1.2. Social impacts

Impact on security and EU citizens (++)

Each of the preferred Sub policy options contributes individually to strengthening EU internal security. When implemented together, their effects are cumulative and mutually reinforcing because they address **successive steps** of cross-border law enforcement cooperation. Improved access to and usability of data (Sub policy options 1.1, 2.1, 2.2, 1.4) strengthens the information base for investigations. Stronger cooperation between EU actors (Sub policy options 1.3, 2.3) ensures that this information can be operationally used and followed up at EU level. Modern digital tools and infrastructure (Sub policy option 2.4) enable this information sharing and cooperation to take place efficiently at scale.

Administrative impacts on national authorities (++)

While some adjustments and implementation efforts will be required, the preferred package is expected to reduce administrative burden over time by simplifying information exchange, improving legal clarity and enabling more efficient operational cooperation. This contributes to greater operational effectiveness and strengthens the capacity of national authorities to address increasingly complex and digitalised criminal threats.

Youth impacts (0)

The preferred option is not expected to have direct impacts specifically targeting young people. However, by strengthening the Union's capacity to prevent and combat serious crime, including offences that particularly affect minors, such as child sexual exploitation

[134] For more details see Annex 3.

and cyber-enabled crime, the measures may have indirect positive effects on the protection and safety of young people across the Union.

8.1.3 Fundamental rights impacts

Objective of general interest (++)

The preferred package makes a significant contribution to the objective of general interest of preventing, detecting and investigating serious and organised crime and terrorism in the Union. By enabling earlier identification of cross-border criminal activities and facilitating more effective operational responses, the measures strengthen the Union's overall capacity to protect citizens and address evolving security threats.

Protection of personal data (0)

Necessity

Some elements of the preferred package increase Europol's ability to query and analyse operational data in support of cross-border investigations (notably Sub policy options 2.1 and 2.4), which may lead to a greater operational use of personal data. At the same time, the reform of data subject categorisation (Sub policy option 2.2) is necessary to address operational inefficiencies that currently limit the effective use of lawfully collected information. Together, these measures enable more timely and effective analysis of data relevant to serious and organised crime and terrorism.

Proportionality

The impact on data protection remains limited and proportionate. The measures do not introduce new categories of personal data. Processing would remain subject to the safeguards provided under the EU data protection framework, including purpose limitation, access controls and independent supervision.

Conclusion

Overall, the preferred package enhances Europol's analytical capabilities while remaining within existing data protection safeguards. Its impact on personal data is therefore limited and proportionate.

8.1.4 Environmental impacts (0)

The preferred option is not expected to have direct environmental impacts. However, by strengthening the operational capabilities of law enforcement authorities to investigate environmental crime, the package may indirectly contribute to the protection of the environment.

8.1.5 Feasibility (+)

All preferred measures are technically feasible as they build on existing legal frameworks, operational practices and IT infrastructure at EU and national level[135].

From a technical perspective, the reform primarily relies on upgrading and integrating existing systems rather than creating entirely new architectures. Synergies with established EU technological frameworks, including those developed by eu-LISA, further enhance feasibility by leveraging proven interoperability standards and secure digital infrastructure.

From a political perspective, the preferred package remains proportionate and compatible with the current distribution of competences between the Union and the Member States.

8.1.6 Impact on digitalisation (++)

The preferred option strongly supports the digital transformation of EU law enforcement cooperation.

Improved data availability and harmonised rules enhance information exchange and operational analysis, while the EU Police Cloud provides the scalable digital infrastructure necessary for advanced analytical capabilities and secure collaboration across Member States.

8.2.REFIT (simplification and improved efficiency)

In line with the Commission's Regulatory Fitness and Performance Programme (REFIT), revisions of existing EU legislation aim to simplify rules and reduce unnecessary administrative burden. In this context, the revision of the Europol legal framework seeks to **streamline procedures** and improve the efficiency of EU law enforcement cooperation.

While the preferred option may require additional engagement from Member States, notably in authorising Europol to query certain national databases and ensuring connectivity to shared services, these efforts are offset by improved operational support, faster cross-border investigations and more efficient use of EU-level analytical capabilities. In particular, the simplification of DSC (Sub policy option 2.2) will directly contribute to reducing administrative burden by introducing clearer procedures and more proportionate safeguards. Additional measures, such as technical guidance, training and centralised support provided by Europol, will further facilitate implementation.

8.3.Application of the 'one in, one out' approach

This initiative **does not impose administrative costs on businesses** and therefore does not trigger the 'one in, one out' adjustment mechanism. The measures primarily concern public authorities involved in law enforcement cooperation and do not introduce new regulatory obligations for the private sector. As a result, the initiative does not entail administrative costs or savings for businesses and does not generate direct costs for citizens. Any adjustment costs associated with the implementation of the preferred option will mainly concern public authorities, notably in relation to the adaptation of information systems and operational procedures.

[135] For example, the Prüm II framework.

At the same time, the initiative is expected to generate significant public benefits by strengthening the Union's capacity to prevent and combat serious and organised crime.

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

The Commission will monitor the impacts of the preferred option through the **existing evaluation and reporting framework under Article 68 of the Europol Regulation**, which provides for periodic assessments of Europol's effectiveness, efficiency and EU added value. To ensure coherence and avoid duplication, monitoring will rely primarily on Europol's established reporting tools[136], complemented where necessary by indicators aligned with the objectives of this initiative.

Monitoring will cover outputs, results and broader impacts, including improvements in information exchange, operational support to cross-border investigations, including the provision of modern capabilities, and inter-agency cooperation. Particular attention will be given to data protection compliance, proportionality and fundamental rights safeguards, including supervision by the EDPS. Indicators will be collected annually from the entry into force of the revised Regulation.

In line with Article 68 of the Europol Regulation, the Commission will carry out an evaluation four years after the entry into force of the revised Regulation to assess its effectiveness, efficiency, coherence, relevance and EU added value, and to inform any future revision. Detailed monitoring indicators are set out in Annex 6.

[136] Including the Consolidated Annual Activity Report, SIENA and EIS reporting, reporting on Member State contributions under Article 7(11) of Europol's Regulation, and Management Board performance indicators.

ANNEX 1: PROCEDURAL INFORMATION

LEAD DG, DECIDE PLANNING/CWP REFERENCES

The lead DG is the Directorate-General for Migration and Home Affairs (DG HOME). The agenda planning (Decide) reference for the Proposal for a Regulation on Europol is PLAN/2025/524.

ORGANISATION AND TIMING

The initiative is planned for Q2 2026 by the Commission Work Programme 2026.

The Interservice Steering Group (ISSG) on the Revision of Europol co-chaired by SG and HOME was composed of the following further services: SJ, BUDG, CNECT, EEAS, ENEST, FISMA, FPI, HR, IAS, INTPA, JRC, JUST, MARE, MENA, OLAF, RTD,TAXUD.

The ISSG on the Revision of Europol met four times to discuss the preparations for the upcoming initiative, namely on 11 April 2025, 11 December 2025, 11 February 2026 and 10 March 2026.

At the meeting of 11 April 2025, the ISSG discussed about the upcoming initiative and the terms of reference for an external study supporting the back-to-back evaluation of the Europol Regulation and the impact assessment for its revision.

At the meeting of 11 December 2025, after the draft interim report of the external 'Study supporting the evaluation and the impact assessment of the Europol Regulation' was presented by the contractor, focusing on the findings of the evaluation, the ISSG discussed the Commission report delivered pursuant to Article 68(3) of the Europol Regulation and the draft intervention logic for the upcoming legislative initiative prepared by DG HOME.

At the meeting of 11 February 2026, the ISSG discussed a very preliminary draft of sections 1-5 of this Impact Assessment report (SWD) to allow the Commission services to discuss and agree on the problem definition, objectives and policy options. DG HOME later shared a consolidated version of the draft SWD to allow the ISSG to comment in writing by 4 March 2026.

At the meeting of 10 March 2026, after the draft final report of the external 'Study supporting the evaluation and the impact assessment of the Europol Regulation' was presented by the contractor, the draft SWD was discussed by the ISSG.

Throughout the process, the ISSG was involved in all key intermediate steps: e.g., Call for Evidence, consultation strategy, public consultation questionnaire, targeted surveys, inception report of the external study, etc.

CONSULTATION OF THE RSB

DG HOME has prepared this draft SWD for submission to the Regulatory Scrutiny Board (RSB) on 18 March 2026 with a view to the meeting with the RSB scheduled for 15 April 2026.

An upstream meeting with the RSB took place on 9 January 2026 to discuss the preparation of the impact assessment accompanying the revision of the Europol Regulation. The discussion focused in particular on the problem definition and evidence base, the distinction between problem drivers and consequences, the operationalisation of objectives in SMART terms, and the design and comparison of policy options. Particular attention was given to fundamental rights and data protection impacts, the coherence of Europol's role within the broader EU security and justice architecture, and the need for robust observational data and cost-benefit analysis. The RSB also provided guidance on strengthening the intervention logic, monitoring framework and overall reader-friendliness of the report.

In line with the recommendations contained in the RSB's positive opinion with reservations, the report has been revised to address all shortcomings identified by the Board. The table below summarises the recommendations made by the RSB and the actions taken to reflect them in the revised Impact Assessment report:

RSB recommendation	Changes introduced in the revised IA report
1. Improve assessment of impacts on fundamental rights, data protection and cybersecurity. Clarify safeguards and mitigation measures.	The section on fundamental rights was substantially revised. The assessment now explains in practical terms how safeguards would operate for each relevant measure, including purpose limitation, access controls, role-based access management, logging, audit trails, retention periods, prior Member State authorisation, EDPS supervision and judicial remedies. A dedicated assessment of cybersecurity risks linked to the EU Police Cloud was added, covering risks such as unauthorised access, data breaches, insider threats, supply-chain vulnerabilities and cloud concentration risks, together with mitigation measures including security-by-design, encryption, zero-trust architecture, multi-cloud deployment, continuous monitoring, and incident response mechanisms.
2. Better explain Europol's legal and operational environment and justify the need for a new reform following the 2022 reform.	The problem definition and baseline sections were strengthened to provide a clearer overview of Europol's position within the EU internal security architecture and its interaction with Member States, Eurojust, EPPO, OLAF and other EU actors. Additional explanation was added to demonstrate that many operational challenges stem from developments that occurred after the adoption of the 2022 reform, including the rapid increase in data volumes, digitalisation of crime, operational experience with the amended mandate, emergence of new technologies and implementation lessons learned since entry into force.

3. Better distinguish regulatory, operational and resource-related drivers and strengthen evidence base.	he problem tree and problem description were revised to clearly distinguish between regulatory constraints, operational limitations and resource/capacity-related challenges. Additional evidence and operational examples were incorporated throughout the report, including Europol operational statistics, SIENA and Europol information system usage data, EPPO cooperation figures, information exchange indicators and findings from evaluations and stakeholder consultations.
4. Reformulate specific objectives in SMART terms and strengthen links to policy options.	The specific objectives were revised following SMART principles. Objectives are now formulated in a more measurable and operational manner. The intervention logic was strengthened by clarifying the link between identified problems, specific objectives, operational objectives and the corresponding sub-policy options. Explanations were added throughout the policy options chapter to demonstrate how each measure contributes to achieving the objectives.
5. Better define policy measures, including cooperation with Eurojust and the EU Police Cloud.	Additional operational detail was introduced for several measures. For Europol-Eurojust cooperation, the report now explains how the enhanced hit/no-hit mechanism would function in practice, including automation and information flows. The EU Police Cloud description was substantially expanded, including architecture, access model, data processing environment, analytical tools, interoperability features, cloud infrastructure, digital identity framework, APIs and operational safeguards.
6. Improve cost assessment and ensure consistency across the report.	The costing methodology was revised and harmonised across the report and annexes. The assessment now clearly identifies the reference period as the 2028-2034 MFF. Cost tables distinguish one-off and recurrent costs and present cumulative costs over the MFF period. Explanatory text was updated throughout the report to consistently refer to annual and cumulative costs. The nature of costs was clarified as implementation/adjustment costs rather than administrative burden. Cross-references and calculations were aligned between the main report and Annex 3.

7. Strengthen monitoring and evaluation framework and link objectives to indicators, outputs, outcomes and impacts.	The monitoring framework was comprehensively revised. Indicators are now explicitly linked to specific objectives and operational objectives. The framework distinguishes outputs, outcomes and impacts and introduces measurable performance indicators. Additional indicators were added covering information exchange, operational support, cooperation with EU agencies, deployment of capabilities, uptake of systems and user satisfaction. Targets and measurement approaches were clarified to facilitate future evaluation of effectiveness, efficiency and impact.

EVIDENCE, SOURCES AND QUALITY

The impact assessment is based on the results of an inclusive and comprehensive consultation of all relevant stakeholders (Annex 2), which equally informed the evaluation of the Europol Regulation (Annex 7). The consultation included scientific expertise, for instance through four expert workshops[137]. Consultations[138] and desk research were conducted also in the context of the 'Study supporting the evaluation and the impact assessment of the Europol Regulation', which contributed to the evidence base for this back-to-back evaluation and impact assessment[139]. Observational data complement stakeholder views, reinforcing the evidence base.

[137] See Annex 2.
[138] Ibid.
[139] The draft final report of March 2026 was submitted to the RSB together with the draft of this SWD.

ANNEX 2: STAKEHOLDER CONSULTATION (SYNOPSIS REPORT)

1. Introduction

The preparation for the upcoming legislative proposal on Europol has been anchored in an inclusive and comprehensive consultation of relevant stakeholders to ensure that the proposal reflects both the political ambition to reinforce Europol[140] and the operational needs of the Member States.[141]

In line with the Better Regulation Guidelines and Toolbox, this annex provides an overview of the stakeholder consultation activities undertaken in preparation for the initiative. It summarises the consultation strategy, the stakeholders consulted, the consultation methods used, the main views expressed, and how these views have been taken into account in the preparation of the impact assessment.

2. Consultation strategy

The consultation strategy followed three main phases. The first phase served to discuss extensively with the Member States at policy and senior official level to adequately scope their operational needs (May – June 2025). The second phase served to gather in-depth feedback and evidence from all relevant stakeholders, including on both the evaluation of the Europol Regulation and all the elements of the impact assessment, ranging from the definitions of the problems and objectives to the analysis of the impacts of the policy options and the comparison of policy measures (July 2025 – February 2026). The third phase served for discussions at political level (March 2026).

3. Consultation activities

3.1 Phase 1: extensive consultations with the Member States at policy and senior official level

Scoping discussions with the Member States were held in multiple fora, notably:

- the EU Council Standing Committee on Internal Security (COSI);

- the High-Level Forum on the Future of EU Criminal Justice;

- the Management Board of Europol;

- the consultation kick-off meeting organised by DG HOME at senior official level;

- the EU Council Law Enforcement Working Party (LEWP).

---

[140] See Political Guidelines for the Next European Commission 2024-2029 & ProtectEU.
[141] Joint Statement by the European Police Chiefs on the Future Development of Europol.

Regarding the outcomes of these consultations, Council discussions in COSI and LEWP showed Member States broadly support reinforcing Europol's operational role within the current treaty limits, while strongly rejecting the idea of a "European FBI" and being concerned about including hybrid threats as a crime area for which Europol is competent. At the High-Level Forum on EU Criminal Justice of 21 May 2025, judicial authorities also expressed support for strengthening Europol's core tasks, particularly data exchange and support for the EPPO. At the consultation kick-off meeting organised by DG HOME on 20 June 2025, Member States expressed consensus on increasing Europol's operational effectiveness without transforming it into an executive or intelligence agency. They prioritised faster, more flexible support for national investigations. They cautioned against centralising expertise at the EU level alone. The dedicated discussion in the Management Board of Europol on 25 June 2025 revealed Member States' support for reinforcing Europol's role as the EU criminal information hub, improving processing of large data sets and addressing legal and technical obstacles in the data protection framework.

3.2 Phase 2: In-depth evidence gathering

3.2.1 Call for evidence

The Commission published a call for evidence on the 'Have your say' web portal from 3 July 2025 to 31 July 2025. Seventeen valid responses were received. Six position papers were submitted by business associations, non-governmental organisations (NGOs) and academia.

Table – Responses to the call for evidence by stakeholder group and country of origin

Stakeholder group	Country of origin	Number of responses
Academic/research organisation	Romania	1
Business association	Belgium	3
Company/business	Austria, Italy	2
EU citizen	Belgium, Bulgaria, Finland, Germany, Lithuania, Slovakia	6
Non-EU citizen	Mexico	1
Non-governmental organisation (NGO)	Belgium, United Kingdom	2
Trade Union	Belgium, Luxembourg	2

Total		17

The main points raised by the respondents to the call for evidence:

- General support for strengthening Europol's mandate, particularly to address emerging threats, with many calling for enhanced operational capabilities, specialised units, and a stronger coordinating role at EU level.
- Concerns regarding fundamental rights raised mainly by a digital rights NGO and some EU citizens.
- Emphasis on the need to support frontline policing, with police trade unions stressing that any mandate changes should be accompanied by investments.
- Diverging views on the extent of Europol's operational autonomy, with business associations and an environmental NGO favouring stronger operational powers to serve sectoral priorities, while other stakeholders believe Europol should remain primarily a coordination and support body.

3.2.2 Public consultation

The Commission conducted a public consultation on 'Law enforcement cooperation – new Europol regulation (proposed)' via its 'Have Your Say' web portal for 12 weeks, between 27 October 2025 and 15 January 2026. The public consultation aimed to gather insights on: (i) the implementation of the Europol Regulation, focusing specifically on its effectiveness, efficiency, relevance, coherence, EU added value and impact; (ii) existing needs and gaps; (iii) quantitative and qualitative inputs to support the Commission in identifying possible policy measures to support Member States; and (iv) the effectiveness and operational functioning of existing EU tools. The consultation received 33 valid replies. No coordinated campaigns were identified. Eight position papers were submitted by three NGOs, one EU citizen, one public authority, one business association, one company/business, and one stakeholder that identified as "other".

Table – Responses to the public consultation by stakeholder group and country of origin

Stakeholder group	Country of origin	Number of responses
EU citizen	France, Germany, Ireland, Italy, United Kingdom	6
Business association	Belgium	1
Company/business	Belgium, Ireland, United States	3
Consumer organisation	Italy	1
Non-governmental organisation (NGO)	Belgium, United Kingdom	4

Public authority	Croatia, Cyprus, Ireland, Italy, Germany, Netherlands, Norway, Spain, Switzerland	13
Other (not specified)	Germany, Italy, Latvia	5
Total		**33**

The main points raised by stakeholders in the public consultation were as follows:[142]

- **Overall effectiveness is assessed positively, with strong performance in core analytical and coordination functions.** Respondents generally viewed Europol's performance under the current Regulation as effective, particularly its role as the EU criminal information hub, its analytical outputs (e.g. threat assessments and situation reports), and its coordination of investigative and operational actions. At the same time, uncertainty remained higher for cooperation with the private sector and for the development of centres of expertise, and legal factors were most often identified as obstacles to effective implementation.
- **The Regulation is considered relevant to and aligned with EU priorities, with high satisfaction for operational and technological support.** Most respondents judged Europol's objectives and activities to be highly relevant or relevant to EU law enforcement and security priorities. Europol's focus on key crime areas was seen as broadly aligned with EU priorities, and satisfaction was particularly high regarding operational investigative support and technological expertise (including digital forensics, AI-based data analysis and biometrics). There was limited appetite, or uncertainty, about expanding Europol's focus to additional crime areas.
- **EU added value is widely recognised**. An overwhelming majority of respondents rated Europol's EU added value positively, and more than half observed positive changes attributable to the Regulation. In the absence of Europol, respondents considered that Member States would only be able to conduct comparable investigations and information exchanges to a limited extent.
- **Implementation challenges relate mainly to resources, governance and legal–technical constraints.** While respondents generally considered that the current Regulation enables Europol to fulfil its mandate, governance, oversight, and resources received the lowest positive ratings. More broadly, legal and procedural uncertainties (notably regarding access to data and admissibility of evidence), technological and legal disparities between Member States, and rapidly evolving digital criminal methods were identified as significant constraints on effective implementation.
- **Preferred pathways for revision** favour non-legislative measures and targeted

[142] For further information, see the factual summary report of the public consultation registered under Ares(2026)2806442 and published at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Law-enforcement-cooperation-new-Europol-regulation-proposal-/public-consultation_en.

amendments rather than a full mandate overhaul.

3.2.3 Four thematic workshops on the future of Europol

DG HOME organised four thematic workshops on the future of Europol to gather feedback at technical level notably from Member States' experts. Europol participated in all workshops and the EPPO participated in the agenda point on Europol-EPPO cooperation. Each workshop was attended by around 100 experts. Overall, nineteen agenda topics were addressed and around a dozen written contributions by Member States were received by the Commission as a follow-up to the discussions.

The first two workshops were held on 6 and 7 November and were dedicated to "Optimising Europol's data ecosystem and strengthening Europol's role as the EU's operational information hub" and "Developing EU-level specialised law enforcement expertise and operational innovation within Europol, and reinforcing Europol's role in tackling persistent and emerging security threats, including within the EMPACT framework". The third and fourth thematic expert workshops were held on 18 and 19 December and were respectively dedicated to "inter-agency cooperation, notably strengthening law enforcement and judicial cooperation with the EPPO" and "resources, Europol's human resources model, governance and data protection".

On optimising Europol's data ecosystem and strengthening Europol's role as the EU's operational information hub, experts agreed on the need to upload, securely share and jointly analyse large sets of data in real-time. They stressed the need to have joint and simultaneous data analysis, paving the way towards a collaborative EU law enforcement digital space, as a one-stop-shop working environment. They emphasised the need to bolster Europol's capacities to cooperate with private parties. Experts expressed varying degrees of openness to a more active role for Europol in accessing existing information at both national and EU levels.

On strengthening Europol's operational role in coordinating support to counter persistent threats, a majority of experts considered that the operational mechanisms already in place (OTFs, EMPACT) work well and require only additional funding to respond to their needs. Experts did not consider medium or long-term deployment of Europol staff (e.g. the European Operational Team Costa del Sol) necessary, but supported targeted and flexible deployments, if required, and upon request by Member States.

On enhancing EU-level specialised expertise in fighting online crime, experts emphasised the operational need to enhance Europol's supportive role in the "digital space". They underlined the benefit of technical standardisation and discussed on an enhanced role for Europol in case the national authority cannot be identified.

On reinforcing Europol's support role in countering emerging criminal threats, experts

agreed that Europol's capabilities should focus on the criminal law component. They did not propose adding hybrid threats as part of the forms of crime for which Europol is competent, noting that the current list of crimes already provides sufficient scope for requesting Europol's support in response to their operational needs.

On strengthening EPPO-Europol cooperation for greater operational impact, discussions highlighted the growing demand for Europol support to EPPO investigations. EPPO called on moving from constrained information sharing toward full bidirectional information exchange, reinforced analytical capacities at Europol, possible dedicated structures for EPPO-related crime areas, and operational support on the ground with Member States' consent. While Member States broadly supported stronger operational cooperation, views diverged on creating dedicated Europol units and on legal changes. Many experts favoured fully exploiting the existing legal framework, stressing data ownership principles and better coordination.

On building a stronger EU law enforcement-judicial cooperation continuum, there was a broad agreement on the added value of OTFs and JITs and on the need for enhanced Europol support, including training, coordination, and deconfliction. Member States called for simplified procedures and increased financial resources. Strong support was expressed for the EU-funded SIRIUS project and for establishing a permanent joint Eurojust-Europol platform, notably for asset recovery, including crypto assets.

On enhancing information sharing and aligned information management, Member States reaffirmed SIENA as the core secure communication channel and underlined the need to harmonise the inter-agency legal framework to avoid duplication, particularly between Europol and Frontex. Some supported broader information exchange with other EU actors, including AMLA, ENISA, the ECB (on terrorism) and MAOC-N (on maritime drug trafficking).

On joining forces in digital services and cloud solutions, there was broad support for developing a secure, future-proof EU cloud solution to enhance data management and joint processing. Different options were discussed, ranging from a private Europol cloud provided by a European supplier to a common eu-LISA-hosted infrastructure for the JHA domain. Experts agreed on the strong operational need and on the necessity for further reflection on the most appropriate model.

On Europol's data protection framework, Member States widely considered data protection rules, as currently interpreted, to be a major operational constraint. Many supported a review of Europol's data processing powers, notably for uncategorised data, with a shift towards a case-based approach aligned with national practices, while maintaining a high level of protection. Simplification of procedures and a review of data retention periods were also advocated, particularly in light of the EDPS' strict interpretation.

On strengthening Member States' role in Europol governance, experts agreed on reviewing the functioning of the Europol National Units (ENUs) and strengthening their role as the key interface between Europol and national authorities. ENUs should be empowered act as a national "mirror" of Europol, enhancing awareness, trust and effective use of the Agency's tools.

3.2.3 Targeted consultations in the context of the external supporting study

An external study was commissioned to support the preparation of the initiative. It started in July 2025. The contractor carried out extensive consultation activities until March 2026. Notably, these included six targeted surveys, more than 135 stakeholder interviews (12 exploratory interviews followed by more than 123 targeted interviews), six field visits, and three focus group meetings.

The targeted surveys were developed for the following stakeholder groups:

1. National law enforcement authorities of the EU Member States.
2. National law enforcement authorities of third countries.
3. Law enforcement networks.
4. EU agencies, bodies and offices (BOAs).
5. Private parties- companies.
6. Non-governmental, civil society and research organisations.

Interviews were conducted with:

- national authorities of the EU Member States, including Denmark (56);
- Europol staff members, including managers and senior managers (35);
- European Commission services (14);
- EU agencies[143] (8);
- EU bodies and offices[144] (4),
- law enforcement networks[145](6);
- MAOC-N;
- third countries[146] (4)
- international organisations[147](1);
- the private sector[148] (2)

[143] CEPOL, EIGE, EUDA, eu-LISA, Eurojust, Frontex.
[144] EEAS, EPPO, OLAF, EDPS.
[145] AIRPOL, ATLAS, EIFS, ESG, HRSN, RAILPOL.
[146] Australia, Brazil, Switzerland, Türkiye.
[147] Interpol.
[148] European Banking Federation; FEPORT.

- youth organisations[149] (1).

The field visits took place in Europol and five Europol Member States.[150]

The three focus group meetings were dedicated to:

1. national authorities of the EU Member States, including Denmark;
2. EU agencies and bodies for internal security, in line with ProtectEU;
3. Europol.

The **targeted survey for the national law enforcement authorities of the EU Member States** received 109 responses from 24 out of 25 Europol Member States and can thus be considered as highly representative[151]. Most responses were received from Germany (50), Finland (7), Belgium and Italy (6). Responses were received mostly from international police cooperation units (61%) and home affairs ministries (48%).

The main points raised by survey respondents:[152]

- **Key evaluation findings:** Europol is widely assessed as effective, relevant, and providing strong EU added value, particularly in supporting cross-border information exchange, operational coordination, and investigations, though relevance is more mixed in areas such as training, innovation, and certain emerging domains.
- **Implementation challenges:** Key challenges include legal and procedural constraints on information sharing, uneven data contributions and follow-up among Member States, limited automation and interoperability between Europol systems and national databases, resource constraints, administrative and financial burdens, and variable awareness or uptake of certain Europol tools and innovation outputs.
- **Pathways for revision:** Forward-looking preferences prioritise increased resources, improved data sharing and interoperability, enhanced analytical and technical capacity, stronger training and capacity building, and clearer coordination with other EU agencies. Support for legislative changes is cautious and focusing mainly on expanded analytical and data-processing capabilities rather than broad mandate expansion.

[149] Missing Children Europe.
[150] Austria, Italy, The Netherlands, Slovenia, Sweden.
[151] Germany, Finland, Belgium, Italy, Hungary, Bulgaria, Czechia, Latvia, Austria, Romania, Estonia, Portugal, Slovenia, Croatia, Cyprus, France, Ireland, Lithuania, Luxembourg, Malta, Netherlands, Poland, Slovakia, Sweden, noting the 109th response from the 24th Europol Member State was received much later than the deadline for replies and has therefore still to be included in the report produced by the contractor.
[152] Due to the large number of responses from Germany (50) and as several other countries also provided multiple replies, the data was cleaned and collated at a country level to provide a single aggregated response per Member State. For each country, averages or sums were calculated across all the quantitative questions, and if any options in a multiple-choice question were selected this counted as a response.

The **targeted survey for EU BOAs** received 13 responses, namely from all the EU justice and home affairs agencies concerned[153], "EU agencies and bodies for internal security" of direct relevance to the implementation of ProtectEU[154], and two more[155].

The main points raised by survey respondents:

- **Key evaluation findings:** Cooperation with EU Agencies is generally seen as strategically effective and aligned with EU security objectives. Europol's activities are broadly relevant to agency mandates, particularly for EU-level coordination, but vary in operational impact depending on mandates and working arrangements. Overall, Europol provides strong EU added value as a central hub for information, analysis, and cross-border support, complementing the roles of other EU Agencies.
- **Implementation challenges:** Key challenges include gaps in the timeliness and completeness of information sharing (notably with Eurojust).
- **Pathways for revision:** Forward-looking considerations prioritise strengthening and updating existing cooperation frameworks rather than structural overhaul, with emphasis on more systematic information sharing, enhanced analytical and operational capacity, improved resourcing, streamlined contact points, and expanded joint work, including through the EU Innovation Hub for Internal Security.

The **targeted survey for national law enforcement authorities of third countries** received 22 individual responses[156].

The main points raised by survey respondents:

- **Key evaluation findings:** Cooperation with third-country authorities is generally seen as effective, particularly in cybercrime, drug trafficking, operational analysis, SIENA-enabled information exchange, joint operations, and training, with strong recognition of Europol's role in addressing evolving criminal methods. Europol's support is broadly aligned with third country needs, although relevance is weaker in terrorism-related cooperation and some innovation areas. Overall, Europol delivers clear EU added value by enabling cooperation with Member States, strengthening cross-border data exchange and analysis, and providing coordination and intelligence capabilities that would be difficult to achieve independently.
- **Implementation challenges:** Key challenges include legal and data protection constraints on information sharing, limited or absent direct access to Europol data and systems (notably for Schengen Associated Countries), operational needs falling outside the scope of existing agreements, resource constraints, and occasional delays in feedback or request processing.

[153] CEPOL, EIGE, eu-LISA, EUAA, EUDA, Eurojust, FRA, Frontex.
[154] ENISA, EPPO, OLAF.
[155] ELA, EMSA.
[156] From Albania, Australia, Bosnia and Herzegovina, Brazil, Colombia, Ecuador, Georgia, Iceland, Japan, Kosovo, Moldova, North Macedonia, Norway, Switzerland, Türkiye, UK, Ukraine, USA.

- **Pathways for revision:** Forward-looking preferences prioritise more flexible and inclusive cooperation arrangements, including improved access to Europol systems and operational data, broader participation in analysis projects, JITs and OTFs, strengthened analytical and training capacities, and targeted adjustments to cooperation frameworks to address emerging threats and close operational gaps for associated and partner countries.

The **targeted survey for law enforcement networks** received 20 individual responses.

The main points raised by survey respondents:

- **Key evaluation findings:** Cooperation with Europol is generally seen as effective, particularly in coordination and support through information sharing, analysis, and innovation tools, although some note greater operational coordination is expected. Europol's activities are broadly relevant to European law enforcement networks, especially in analysis, coordination, and innovation, but vary depending on mandate fit and operational needs. Overall, Europol provides strong EU added value as a central hub for intelligence, secure information exchange, analytical capacity, innovation, and cross-border coordination.
- **Implementation challenges:** Key challenges include legal and procedural barriers to information sharing, delays or gaps in operational data exchange, limited analytical and technical capacity, resource and funding constraints, administrative burdens.
- **Pathways for revision:** Forward-looking preferences prioritise strengthening practical support rather than wholesale redesign, including simplified administrative and funding procedures, improved information-sharing tools, enhanced analytical and operational capacity, clearer mandate alignment with network needs, and more structured, long-term support, with mixed views on mandate expansion balanced against preserving network autonomy.

The **targeted survey for private parties- companies** received 20 responses, almost entirely from companies which are known to cooperate with Europol.

The main points raised by survey respondents:

- **Key evaluation findings:** From the private sector perspective, cooperation with Europol is generally effective, particularly in information sharing, operational collaboration, and established public–private partnerships, though effectiveness is less clear in research and innovation activities. Europol's engagement is broadly relevant, especially in financial services and cybersecurity, but varies across sectors due to uneven awareness and involvement. Overall, Europol provides strong EU added value as a central hub for cross-border coordination, intelligence, and public–private cooperation, delivering capabilities and scale beyond national efforts.

- **Implementation challenges:** Key challenges include legal constraints on information sharing, limited clarity on Europol's specific intelligence needs and feedback mechanisms, fragmentation and technical limitations of information sharing platforms.
- **Pathways for revision:** Forward-looking preferences focus on strengthening and scaling existing cooperation models rather than structural overhaul, with emphasis on clearer guidance and legal certainty, more specialised and secure information-sharing platforms, enhanced operational collaboration and feedback loops, improved resourcing of successful partnerships, and governance arrangements that ensure transparency and standardisation.

The **targeted survey for non-governmental, civil society and research organisations** received responses from 14 organisations[157].

The main points raised by survey respondents:

- **Key evaluation findings:** Europol's engagement with civil society is effective mainly in targeted, project-based and research-driven areas, while overall effectiveness is harder to assess due to limited interaction. Its activities are generally seen as relevant and coherent with civil society priorities on cross-border crime and analysis, though gaps remain in prevention, victim support, and integrating human and digital rights.
- **Implementation challenges:** Key challenges identified include limited transparency and accessibility of engagement mechanisms, uneven awareness of cooperation opportunities, administrative barriers, and concerns regarding governance, accountability, and the fundamental rights implications of expanded data processing and AI-based analysis.
- **Pathways for revision:** Forward-looking preferences emphasise establishing structured and inclusive engagement with NGOs and civil society, clearer contact points and advisory mechanisms, strengthened transparency and oversight, and reinforced safeguards for fundamental rights.

Field visits to Member States aimed at gathering qualitative, context-specific evidence on Europol's cooperation with Member States.

The main points raised by the interviewees during the field visits to Member States:

- National authorities highly value Europol's role in facilitating cross-border information exchange, analytical support and operational coordination. However, investigative responsibility and judicial accountability must remain at national level, with Europol acting in a supportive and complementary capacity.
- Information exchange is functional but constrained by legal, technical and organisational barriers. Limited interoperability between national systems and

[157] The 14th response was received much later than the deadline for replies and has therefore still to be included in the report produced by the contractor.

Europol tools, reliance on manual uploads and lack of automation create administrative burdens.

- Strict interpretation of data protection provisions is viewed as increasingly burdensome in fast-moving operational contexts, limiting actionable criminal intelligence delivery.
- Europol's strength lies in filtering, contextualising and prioritising information. Proactive identification of cross-border links, emerging phenomena and structured analytical coordination across crime areas were cited as areas where Europol delivers clear EU added value.
- Duplication of analysis across Member States is a as source of inefficiency. There is broad support for stronger interoperability and smarter automation. At the same time, any expansion of access to sensitive data would require mechanisms to maintain trust among Member States.

4. Main horizontal findings of the consultation

4.1 Problem definition

There was broad agreement among stakeholders that Europol and national authorities face persistent information gaps when investigating cross-border crimes and identifying threats, and that Europol's operational support remains limited, including cooperation with EU agencies and EPPO. Information gaps reduce effectiveness in the EU-level fight against serious crime, while operational cooperation faces legal and practical constraints. The current mandate limits Europol's ability to provide optimal support in certain areas.

4.2 Views on strengthening Europol's role

All stakeholder groups recognise Europol's clear EU added value as a central hub for cross-border information exchange, analysis, and coordination that cannot be replicated at national level. Across groups, there is also convergence around the nature of Europol's coordination role as the EU's criminal intelligence hub and as a provider of specialised expertise and analytical support, rather than as an entity replacing national authorities. This includes support for stronger cooperation with partners. Member States are eager to enhance Europol's capacity to support complex cross-border investigations provided that national competences remain respected, clear safeguards for trust-based cooperation are maintained (starting with the data ownership principle) and proportionality is ensured. Conversely, stakeholder views diverged on the extent and modalities of the structural changes required.

5. How stakeholder views have been taken into account

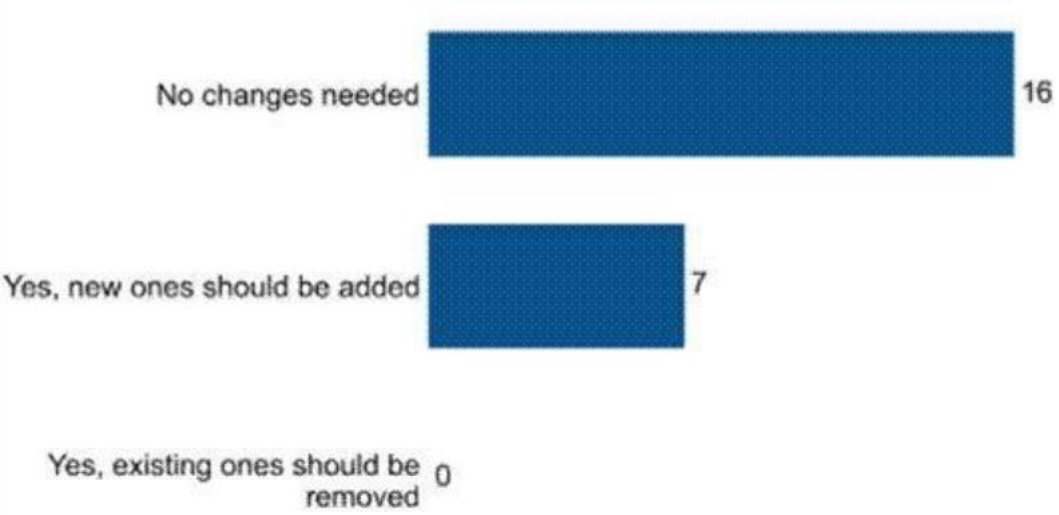
Stakeholders' views informed the initiative throughout the process in several ways. Most importantly, the problem definition and the objectives were refined to reflect the operational needs of the Member States. For instance, the focus group with Europol confirmed information gaps as a primary constraint for the effectiveness of investigations, with Europol's support capacity being limited mainly by uneven and insufficient data

contributions from Member States, and voluntary information sharing approaches having widely reached their limits.

The policy options "reinforcing Europol's existing model" and "a new model for Europol" were tested with the main stakeholders, especially through the focus group meetings, proving effective to capture a wide range of desirable policy measures. Implementation considerations were reflected in the sequencing and design of policy measures. Where views diverged, the impact assessment presents a balanced analysis grounded in proportionality, feasibility and EU added value.

How have stakeholder views been taken into account? A prominent example

Targeted survey for the EU Member States' national law enforcement authorities – Figure 10 – Question 10: ***Are there, in your view, any criminal or security threats or offences that should be added or removed from Europol's mandate to better address current and emerging security challenges?***



16 Europol Member States opposed making Europol competent for new forms of crime, while 8 Europol Member States (7 + 1 late respondent) suggested broadening Europol's mandate by adding new forms of crime to Annex I, especially **hybrid threats**, but also tax crime and others, or by removing the list altogether.

The Commission services took note of Member State experts' position expressed at the thematic workshops that Europol can already provide support to counter the criminal law dimension of hybrid threats insofar as they materialise in any of the several forms of crime for which Europol is competent. Notably, Europol can support crime detection and analysis and coordinate law enforcement responses, which it must do without interfering with the competences of national intelligence agencies.

The Commission services also took note of Member State law enforcement agencies' position expressed over bilateral discussions that, while hybrid threats are transversal in nature, Europol's support against hybrid threats has in practice been provided mostly through a counter-terrorism angle, without fully mobilising Europol's capabilities across all its various operational centres. Europol could instead mobilise the capabilities of all its operational centres to respond to requests from national law enforcement authorities and fully support national investigations, exploiting all its supportive potential under the current mandate, by deploying its entire toolbox in the most relevant crime areas.

This does not require changes to Europol's mandate and has thus been excluded by the impact assessment report.

7. Conclusion

The extensive consultation process confirmed the centrality of the identified problems and the need to adapt Europol's support to evolving security challenges. While stakeholders expressed different levels of ambition regarding structural changes, there was broad recognition of the need to strengthen Europol's support to Member States in tackling serious and organised crime, cybercrime and terrorism. The impact assessment reflects the evidence gathered and seeks to strike a balance between ambition, operational effectiveness, legal certainty and political feasibility.

ANNEX 3: WHO IS AFFECTED AND HOW?

1. PRACTICAL IMPLICATIONS OF THE INITIATIVE

1.1 EU citizens

All preferred options aim to improve the **prevention, detection, investigation, and prosecution of serious and organised crime**, directly benefiting citizens. By enhancing the availability, structure, and usability of law enforcement data, the package supports:

- Earlier detection of cross-border criminal networks.
- Faster identification of suspects and links between cases in multiple Member States.
- Improved asset tracking and coordinated operational responses.
- Stronger protection in both physical and digital environments.

Citizens benefit from a higher level of security while safeguards on data protection and fundamental rights remain fully respected.

1.2 National authorities

a. Law enforcement officers

The initiative equips officers with enhanced operational tools, including:

- Better tools to query data stored in the Europol systems.
- Structured and semi-automated data exchange through integrated national case management systems and the EU Police Cloud.
- Europol support in data processing, analytics and operational coordination, including cross-border investigative leads.
- Clearer and standardised procedures for inter-agency cooperation with Eurojust and the EPPO.

These improvements reduce delays, avoid duplication, and strengthen the quality and timeliness of cross-border investigations.

b. IT organization in Member States

IT teams are affected primarily during initial implementation:

- Initial investment to connect national CMS to Europol platforms and the EU Police Cloud.
- Simplified maintenance and upgrades due to centralised integration, reducing long-term operational burden.
- Streamlined interoperability and harmonised data standards across national and EU systems.

1.3 EU level

a. Europol

- Acts as the central analytical and operational hub for EU internal security, integrating national and EU-level datasets.
- Provides structured operational support to Member States, including intelligence analysis, cross-border link detection, advanced biometric matching and case prioritisation.
- Supports real-time coordination and structured exchange between Member States, EPPO and Eurojust.
- Ensures that national CMS integration and the EU Police Cloud facilitate faster, automated and reliable access to actionable information.
- Delivers scalable technical, digital, and forensic capacity without centralising national data or replacing national investigative powers.

Europol's reinforced role allows for more proactive, timely and consistent support across complex investigations, increasing operational efficiency and EU-wide situational awareness.

b. Eurojust

- Gains access to more structured, reliable, and timely information from Europol to support judicial cooperation and coordination of cross-border prosecutions which facilitates the work of joint investigation teams (JITs) as well as mutual legal assistance requests.
- Benefits from more efficient workflows with Europol information systems.
- Enhanced information quality and timeliness enables more efficient coordination in serious and organised crime cases, strengthening legal certainty and effectiveness of judicial processes.

c. EPPO

- Gains streamlined access to operational data and analytical outputs provided by Europol, enabling quicker decision-making in cross-border prosecutions.
- Strengthened structural partnership with Europol ensures that EPPO investigative needs are systematically integrated into EU-level operational workflows.
- Receives coordinated support in cross-border investigations, including prioritisation of cases, operational insights, and access to enhanced analytical products.
- The partnership improves the quality, consistency, and speed of EPPO-led prosecutions, reinforcing EU-level enforcement capacity while maintaining national procedural autonomy.

2. SUMMARY OF COSTS AND BENEFITS

Cost of the baseline scenario

Unless otherwise indicated, all cost estimates presented in this section are expressed in current prices (2026 EUR) and cover the period 2028–2034, corresponding to the duration of the next Multiannual Financial Framework (MFF). One-off costs refer to implementation and deployment expenditure incurred during the roll-out phase of the

measures, while recurrent costs refer to average annual operational expenditure over the same period. The same methodological assumptions and calculation basis are used throughout the main report and the supporting annexes.

In financial terms, the baseline scenario assumes the continuation of Europol's current funding trajectory without the additional investments associated with the policy options assessed in this impact assessment. Baseline projections are based on the historical evolution of Europol's annual adopted budget between 2017 and 2025 and extrapolated over the 2028–2034 MFF period..

Two projection approaches were considered in order to reflect possible future expenditure patterns.

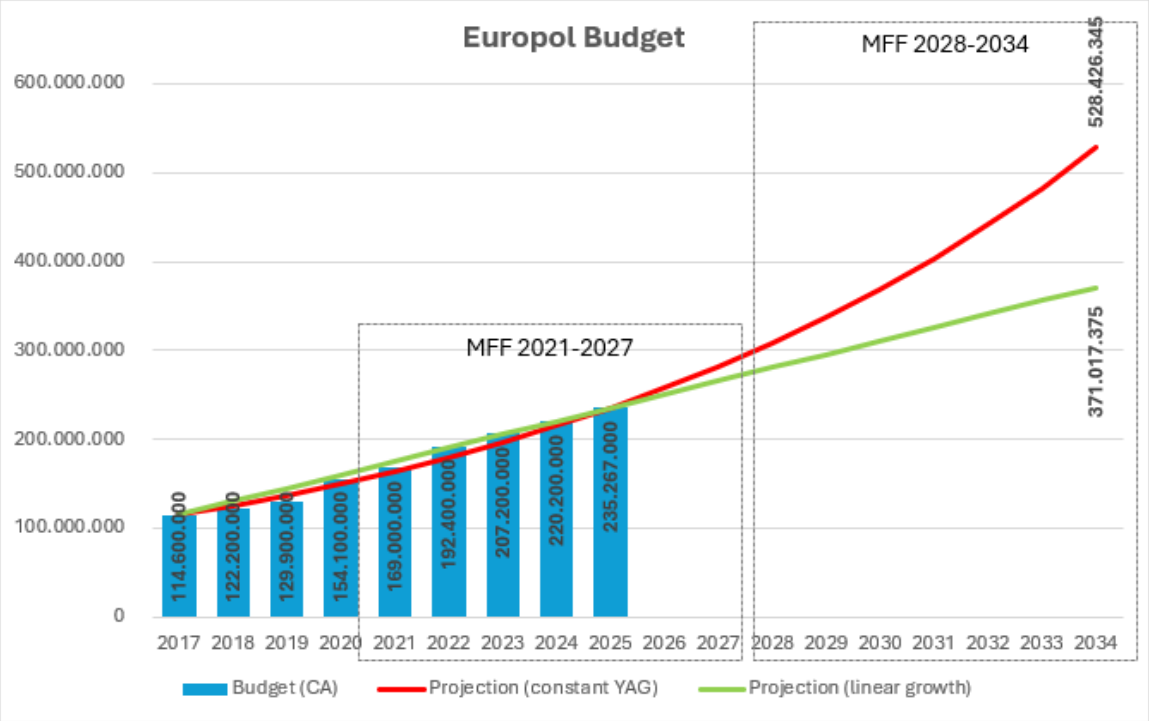
First, a **linear growth scenario** assumes that Europol's budget continues to increase by approximately **EUR 15 million per year**, corresponding to the average annual increase observed between 2017 and 2025. Under this assumption, Europol's total budget over the next Multiannual Financial Framework (MFF 2028–2034) would amount to approximately **EUR 2.28 billion**.

Second, a **constant growth rate scenario** assumes that the historical growth rate observed between 2017 and 2025 continues over the projection period. This corresponds to an annual growth rate of approximately **9.41%**, resulting in a projected budget of approximately **EUR 2.87 billion** over the same MFF period.

For the purposes of the impact assessment, the **linear growth scenario is used as the conservative baseline**, while the constant growth scenario illustrates a possible upper-bound trajectory reflecting the increasing operational demand on Europol.

These projections provide a range for the expected evolution of Europol's budget under the baseline scenario. They reflect the continued expansion of Europol's operational responsibilities and analytical support functions, while assuming no structural changes to its mandate, operational model, or technological infrastructure beyond incremental adaptations within the current framework.

For the purpose of this impact assessment, the baseline therefore assumes a **total Europol budget envelope in the range of EUR 2.3–2.9 billion for the period 2028–2034 (as compared to the current EUR 1.53 billion)**, reflecting the continuation of current trends without the additional investments associated with the policy options assessed in the following section.



Cost of the preferred option

The table below presents the costs associated with the preferred option (in million EUR). One-off costs are presented as cumulative implementation costs over the deployment phase of the preferred option, while recurrent costs cover the cumulated annual average costs during the 2028–2034 period.

No costs are identified for citizens/ consumers and businesses given the costs associated with the policy measures are directed at EU-level or national public administrations.

II. Overview of costs – Preferred option					
		Citizens/ Consumers	**Businesses**	**Administrations**	
		One-off/ Recurrent	**One-off/ Recurrent**	**One-off**	**Recurrent**
Sub policy option 1.1 - ***Data loaders***	Direct costs	N/A	N/A	54 (Member States) 5 (Europol)	75.6 (Member States) 7 (Europol)
Sub policy option 1.1 - ***Upgrade of systems and tools***	Direct costs	N/A	N/A	27 (Member States) 56 (Europol)	37.8 (Member States) 78.4 (Europol)

Sub policy option 1.3 - ***Automation of the Europol-Eurojust hit/ no hit mechanism***	Direct costs	N/A	N/A	0 (Member States) 2 (Europol)	0 (Member States) 7 (Europol)
Sub policy option 1.3 - ***Institutionalisation of SIRIUS***	Direct costs	N/A	N/A	0 (Member States) 0 (Europol)	0 (Member States) 1 (Europol)
Sub policy option 1.4 - ***Europol digital platforms embedded in national investigations***	Direct costs	N/A	N/A	105 (Member States) 50 (Europol)	140 (Member States) 56 (Europol)
Sub policy option 2.1 - ***Access to national databases***	Direct costs	N/A	N/A	0 (Member States) 6 (Europol)	0 (Member States) 30.1 (Europol)
Sub policy option 2.1 - ***DNA matcher***	Direct costs	N/A	N/A	1.35 (Member States) 5 (Europol)	2.1 (Member States) 14 (Europol)
Sub policy option 2.2 - ***Simplified rules to reduce the administrative burden of data subject categorisation***	Direct costs	N/A	N/A	0	0
Sub policy option 2.3 - ***Europol as structural provider of information,***	Direct costs	N/A	N/A	0	0 (Member States) 77.7 (Europol)

analytical support and capabilities to the EPPO					
Sub policy option 2.4 - ***EU Police Cloud***	Direct costs	N/A	N/A	13.5 (Member States) 143.7 (Europol)	4.2 (Member States) 278.6 (Europol)
Sub policy option 2.4 - ***EU Police Digital ID***	Direct costs	N/A	N/A	54 (Member States) 2.5 (Europol)	75.6 (Member States) 3.5 (Europol)
Sub policy option 2.4 - ***Europol support offices***	Direct costs	N/A	N/A	0	0 (Member States) 45.5 (Europol)

All one-off and recurrent costs are implementation costs. No regulatory charges, hassle costs, administrative costs or indirect costs were identified and therefore are not quantified. These are all provisional estimates that would need to be confirmed, including how the costs are split between the different Member States. As a result, the confidence margin of cost estimates cannot be better than 20-25% at this early stage in a project. What is stable is how the costs of the various measures compare with each other. Where precise operational expenditure data were not available, recurring costs were estimated using standard lifecycle costing assumptions derived from comparable EU large-scale IT systems and agency operational expenditure patterns. Unless otherwise specified, annual maintenance and support costs are estimated at approximately 20% of initial deployment costs.

Sub policy option 1.1: Strengthened data availability, processing and service

This option entails upfront investment at both Member State and Europol level, primarily driven by **data loaders as well as system and tools** (including enhance use of interoperability tools).

For **Member States**, one-off costs (EUR 81 million aggregated, approx. EUR 3 million per Member State) relate mainly to:

a) Deployment of **automated data-loader solutions**;
b) Adaptation of national systems to interface with upgraded Europol tools;
c) Integration, testing and limited workflow adjustments;
d) Training of end-users.

The deployment of data-loaders is estimated to range between EUR 1 million and EUR 3 million per Member State depending on the size of the Member States' databases and their level of existing integration. An average of EUR 2 million was therefore taken as a basis.

The remaining EUR 1 million results from the point b) to d). The basis was similar projects in the past where Member States had to integrate workflow adjustments.

Recurring costs (EUR 16.2 million annually, approx. EUR 600 000 per Member State), corresponding to approximately EUR 113.4 million cumulatively over the 2028–2034 MFF period. These costs reflect maintenance, system support and continued operational use. It is calculated as a standard 20% rate of the one-off costs based on similar simulations and building on past experience. Costs remain moderate as the option does **not require entirely new national systems**, but builds on existing infrastructure and voluntary uptake of EU-level services.

For **Europol**, one-off costs (EUR 61 million) are driven by:

- **Major upgrades of core ICT systems** (SIENA, EIS, EAS, QUEST+);
- Development of **centralised interoperability solutions and harmonised data models (UMF)**;
- Design and deployment of standardised data loaders;
- Joint procurement structures and specialised ICT recruitment.

The costs are inspired by similar costs incurred by EU Agencies that built similar technologies. For instance, the cost of building the shared Biometric Matching Service by eu-LISA for the Interoperability Regulations[15820]. The cost figure has been updated from the original 2018 estimate to account for inflation between 2018 and 2026, ensuring that the values reflect current price levels and purchasing power.

Recurring costs are estimated at EUR 11.2 million annually, corresponding to approximately EUR 78.4 million cumulatively over the 2028–2034 MFF period. These costs cover maintenance, cybersecurity, governance, operational support, and reinforced technical and analytical staff. It is calculated as a standard 20% rate of the one-off costs[159].

Although the option requires significant initial investment, it is expected to generate **long-term efficiencies** through:

- Economies of scale via joint procurement;
- Reduced duplication of national developments;
- Europol-supported optimisation and harmonisation of systems.

The financial effort therefore reflects a **structural modernisation of the EU law enforcement information architecture**, with medium- to long-term savings and operational gains.

<u>Sub policy option 1.3</u>: Measure 1 for a reinforced Europol's support to the EPPO

One-off costs for Member States are expected to be negligible or very limited, as the measure concerns the creation of new Europol-level capacities (including a dedicated support unit and time-bound Task Forces) and does not entail structural changes to national

[158] Regulation (EU) 2019/817 & Regulation (EU) 2019/818.
[159] As for instance in the impact assessment accompanying the JITs Collaboration platform – development cost: €8.4 million; annual maintenance and operation: €1.7 million. Ratio: 1.7/8.4≈20%

systems, procedures or staffing. All direct operational, staffing, training and equipment costs are expected to arise at EU level (Europol and, where relevant, EPPO). Any potential impacts on Member States would be indirect and implementation-specific, and no material national cost drivers have been identified.

Recurring costs for Member States are expected to be negligible or very limited, as the measure establishes new capacities at EU level (Europol and EPPO) and does not entail new obligations for national authorities. In particular, the measure does not introduce new duties, workflows, reporting requirements or compliance obligations for Member States, nor does it require contributions of staff, procedural adaptations or the maintenance of additional processes at national level. Any potential impacts on Member States would therefore be indirect and implementation-specific, and no material recurring cost drivers have been identified at this stage.

No separate one-off costs are calculated for Europol, because the costing approach already captures them within the annual cost estimates. Indeed, the annual costs are based on the average resources allocated to Europol officers – a benchmark that already includes salaries, onboarding, training, equipment, and other personnel-related expenses.

The recurrent costs to Europol stem from establishing a dedicated Support Team for EPPO investigations, which requires the long-term employment of additional specialised officers. These staff carry out operational analysis, cross-checks, and digital forensics, and their salaries and related personnel expenses form the ongoing cost driver. Based on projected staffing needs, recurrent costs are estimated to range from EUR 8.7 million in 2028 to EUR 11.8 million in 2034, with an annual average of EUR 10 million, corresponding to an estimated cumulative cost of approximately EUR 70 million over the 2028–2034 MFF period.

Sub policy option 1.3: Measures 2 and 3 for a strengthened continuum of EU-level support to law enforcement cooperation through Europol and judicial cooperation through Eurojust

Both the one-off costs for Member States and the recurring costs for Member States are expected to be negligible, as the measures regard cooperation between Europol and Eurojust and the support they provide to Member States in return.

The measures would largely build on existing technical infrastructure and operational arrangements between Europol and Eurojust. For the hit/no-hit mechanism, precise estimation of direct one-off costs is challenging, as these would depend on the level of technical ambition chosen for automation and the extent of system integration pursued. A light-touch approach focused on enhancing existing interfaces would entail minimal additional expenditure, while more advanced automation solutions could involve moderate investment in system configuration and security. For the SIRIUS Project, the institutionalisation within both the Europol and Eurojust Regulations would not require the creation of new infrastructure – SIRIUS is currently operational and supported by existing systems, workflows and personnel – but rather organisational adjustments, procedural alignment and limited technical refinement.

The automation of the hit/no-hit mechanism is expected to reduce the staff-intensive manual exchanges currently required under the baseline, generating administrative efficiency gains. The recurring costs for SIRIUS are expected to broadly follow the baseline level of resources already devoted to the project, with adjustments reflecting demand and operational scope. This corresponds to estimated recurrent costs of approximately EUR 1 million annually for Europol, or around EUR 7 million cumulatively over the 2028–2034 MFF period.

The institutionalisation of SIRIUS and the upgrading of the Europol–Eurojust hit/no-hit mechanism are expected to generate a minimal positive impact on efficiency compared to the baseline. Under SIRIUS Phase II (2021–2025), the total project budget amounted to approximately EUR 3.49 million over four years (EUR 2.16 million for Europol; EUR 1.33 million for Eurojust), with 7 contract agents supporting its activities at Europol and 4 at Eurojust. Institutionalisation would not necessarily require a substantial increase in resources beyond this envelope but would shift funding from a contribution-agreement model to stable internal budget lines within Europol (and Eurojust), potentially requiring the conversion of contract agents into temporary agents and modest additional administrative overhead.

Regarding the hit/no-hit mechanism, the current manual and template-based model has proven highly burdensome and operationally ineffective, requiring extensive manual verification and layered authorisations for minimal operational output. Of the two possible implementation modes, the person-to-system approach is likely to be more proportionate and immediately feasible from an efficiency perspective, as it limits large-scale data transfers while reducing manual workload and preserving data ownership. The more ambitious system-to-system model could generate higher long-term analytical gains but would entail greater upfront IT development and legal alignment costs. Even if the volume of meaningful hits remains modest, a more automated and scalable mechanism would reduce transaction costs, improve timeliness and increase the likelihood of detecting genuinely relevant cross-case links at an earlier stage.

Sub policy option 1.4: Europol's digital platforms embedded in national investigations

Member States: One-off costs are estimated at **EUR 105 million**, reflecting the implementation of new criminal information strategies that integrate both national and EU-level investigative lifecycles. This includes updating national systems supporting law enforcement procedures, such as CMS, Single Point of Contact CMS and corresponding police records, mapping existing data and workflows to the UMF standard. National workflows will be adapted to integrate systematic use of QUEST+ and data loaders, alongside associated **training and change management** for staff to ensure proper adoption. Recurring costs are estimated at **EUR 20 million per year**, corresponding to around EUR 140 million cumulatively over the 2028–2034 MFF period, covering ongoing operational adjustments, refresher training and maintenance of updated national workflows and IT systems.

Europol: One-off costs are estimated at **EUR 50 million**, covering the **upgrade of central data ingestion components**, including extending Europol Case Management Systems and other databases (e.g. Europol Information System) to handle EU-wide object identifiers and scaling up processing capacities. Costs also include **reinforcement of the dedicated team** responsible for facilitating integration between Europol and national systems, ensuring smooth operational collaboration. Additionally, costs cover **standardisation efforts**, including the development of guidance documents supporting Member States' new criminal information lifecycle strategies. Recurring costs are estimated at **EUR 8 million per year**, corresponding to around EUR 56 million cumulatively over the 2028–2034 MFF period, reflecting ongoing support to Member States, continued maintenance and monitoring of upgraded systems and operational assistance to ensure effective implementation of new workflows and interoperability practices.

Sub policy option 2.1: Europol as an operational service provider and information hub

The first part of the cost assessment focuses exclusively on access via the existing Prüm framework. Under Prüm, Member States' costs remain negligible, as the measure builds on the existing legal and technical architecture and does not require new large-scale IT systems for simple query-only access. According to the Prüm II Impact Assessment[160], establishing technical connectivity (e.g. for DNA matching) has been estimated at around EUR 300 000 per Member State for DNA and similar biometric exchange functionality, reflecting moderate one-off investments for automated integration with existing systems. Consequently, the incremental costs for Member States under Sub policy option 2.1 are considered limited, and estimated to **EUR 50 000 per Member State** as this option does not introduce additional legal access rights nor require complete redesign of national infrastructures.

For **Europol**, costs linked to access to national databases are primarily driven by:

- Additional **forensic experts and operational staff** to follow up on matches, consistent with estimates in the legislative financial statement accompanying proposal for a Prüm II Regulation[161] which foresee staff costs for search verification by EU agencies;
- Reinforcement of **information management capacities** to ensure secure and efficient data flows;
- **Limited system adaptations** to handle increased volumes.

The estimated costs for the EU DNA matcher are informed by operational cost estimates developed by forensic authorities in the context of preparatory work for a pilot project. In particular, a budget proposal prepared by the Netherlands Forensic Institute (NFI) for a two-year pilot project foresees a dedicated project team including forensic experts, IT developers and project management staff, supported by technical infrastructure and

[160] SWD(2021) 379.

[161] COM (2021) 784 final

operational overhead. The budget calculations rely on standard governmental salary scales and include an overhead rate of approximately 25 %, consistent with typical EU project financing structures.

The pilot proposal assumes that most personnel would be employed directly by the participating forensic institute, although additional costs could arise if specialised IT expertise needs to be sourced through subcontracting. Such subcontracting could potentially double certain personnel costs, illustrating the importance of relying on existing institutional capacities where possible. Those costs would be shifted towards Europol in line with sub policy option 2.1. The estimations consider that 75% of the recurring EUR 2 million annual adjustment costs (corresponding to approximately EUR 14 million cumulatively over the 2028–2034 MFF period) would represent HR costs. With the remaining being divided between travel, equipment and other goods and services costs.

These operational estimates confirm that developing and testing a shared EU-level DNA matching capability requires a **relatively limited recurring adjustment cost notably covering HR costs**. The cost assumptions used for Policy Option 2.1 therefore reflect a realistic implementation scenario based on existing forensic cooperation initiatives.

The baseline for this assessment is not zero, as many Member States already rely on third-country based matching solutions managed outside the EU framework. Over time, Union-level costs under this option are expected to be offset by:

- **Reduced duplication of national efforts** in forensic matching and follow-up work;
- **Economies of scale** from shared EU-run services rather than multiple national or external systems;
- **Avoidance of third-country dependency costs** associated with non-EU provider solutions.

The investment therefore represents not only operational reinforcement but also a **long-term strategic consolidation of EU capabilities**.

Sub policy option 2.2: Simplified rules to reduce the administrative burden of data subject categorisation

Policy option 2.2 on DSC would significantly enhance **Europol's operational flexibility** and its capacity to process and analyse information in a timely manner, while **not requiring substantial initial financial investment**. The measure primarily entails **legislative alignment, clarification and simplification of the existing framework**, rather than the development of new IT systems or structural reorganisation. As such, implementation costs would be limited and largely confined to **internal adjustments, updated guidance and targeted training**.

Importantly, the option would reduce or eliminate the **resource-intensive procedures linked to data subject categorisation** under the current framework. Staff time currently devoted to ***ex ante* categorisation, verification and corrective compliance actions** could instead be redirected towards operational analysis and investigative support. This reallocation of resources is expected to generate **tangible administrative savings and**

efficiency gains over time. Overall, the combination of **limited (to no) upfront investment and sustained operational efficiencies** justifies a **very positive cost assessment**, although precise quantification of these efficiency gains remains subject to uncertainty at this stage due to limited comparable operational data.

Sub policy option 2.3: Europol as structural provider of information, analytical support and capacities to the EPPO

The one-off costs for Member States are expected to be **negligible or very limited**, as the measure does not require them to provide additional staff, adapt national systems, or assume operational expenditures. The initiative is designed to operate at EU level, and therefore does not generate structural investment needs at national level. Likewise, **no significant recurring costs** are anticipated for Member States, as they would neither contribute personnel nor cover ongoing operational, administrative or compliance-related expenses linked to the reinforced cooperation framework.

For Europol, no separate fixed start-up costs are identified, since the costing methodology is based on the **average annual cost per staff member**, which already incorporates salaries, onboarding, training, equipment, IT access and other personnel-related overheads. As a result, initial implementation costs are embedded within the overall annual resource envelope.

The recurrent costs for Europol arise primarily from the establishment of a **dedicated Support Team for EPPO investigations**, requiring the long-term employment of additional specialised officers. These staff members would carry out operational analysis, cross-checks, digital forensic support and structured case coordination, with an estimated annual average cost of **EUR 10.1 million,** corresponding to around EUR 70.7 million cumulatively over the 2028–2034 MFF period. In addition, permanent cooperation mechanisms, including reinforced coordination structures and liaison arrangements, would entail further staffing needs, with estimated additional annual costs of **less than EUR 1 million** (less than EUR 7 million cumulatively over the 2028–2034 MFF period). Overall, the financial impact is concentrated at EU level and reflects a structural reinforcement of analytical and prosecutorial support capacities.

Sub policy option 2.4: Measure 1 on the EU Police Cloud

The initial investment costs associated with the deployment of the **EU Digital Police Cloud and the EU Police Digital ID** are substantial, reflecting the scale and strategic nature of the infrastructure.

For Member States, *one-off costs* are estimated at **EUR 13.5 million for the EU Police Cloud**, EUR 0.5 million per Member State to bring national law enforcement ICT infrastructure and criminal investigators' endpoints (laptops, tablets and smartphone) in line with a set of harmonized rules for the technical interoperability and security of applications and digital services, notably when provided on classified networks, and **EUR 54 million for the EU Police Digital ID** (i.e. EUR 2 million per Member State for stepping up the national digital identity scheme for criminal investigators based on a Digital Identity wallet level high, for exhaustively issuing such credentials, and integrating the national police identity scheme within the wider EU digital police scheme). *Recurring costs* of **EUR**

0.6 million per year for the Cloud (approximately EUR 4.2 million cumulatively over the 2028–2034 MFF period) to maintain the national law enforcement ICT architecture up to the evolving common standards and **EUR 10.8 million per year for the Digital ID** (approximately EUR 75.6 million cumulatively over the 2028–2034 MFF period) for the Digital ID to insure the level of authentication against the Police Cloud is maintained over time up to the latest standards and is kept available to the evolving investigators' staff.

For Europol, *one-off investments* amount to **EUR 143.7 million for the EU Police Cloud** which account for the extensive migration of operational data processing operated by Europol to a platform based self-service architecture, (applications such as EIS, analysis projects, biometric identification, crypto asset tracing, OSINT, digital forensics and especially those limited to Europol's analysts) for the establishment of harmonized technical rules applicable to national ICT infrastructures, and for the initial set-up costs of Cloud Services, particularly for classified information and **EUR 2.5 million for the EU Police Digital ID** for renovating Europol's identity and access management (IAM) platform and establishing harmonized rules for national authorities issuing such IDs. *Recurring* costs are estimated at **EUR 39.8 million annually for the Cloud,** corresponding to around EUR 278.6 million cumulatively over the 2028–2034 MFF period**,** to maintain and develop the portfolio of online applications and most importantly for operating the online service and **EUR 0.5 million per year for the Digital ID** (around EUR 3.5 million cumulatively over the 2028-2034 MFF period) for maintaining both the IAM platform and stirring the evolution of common standards on a Police Digital Identity at EU level. These costs cover infrastructure development, secure hosting environments, identity and access management solutions, system integration, data migration, cybersecurity safeguards, and ongoing technical management.

Despite the scale of the initial expenditure, these investments represent a structural modernisation of EU law enforcement digital capabilities. By consolidating processing environments, standardising secure access through a common Digital ID, and reducing fragmentation across disparate national systems, the initiative is expected to generate significant long-term efficiencies. Cost savings will stem from economies of scale, reduced duplication of infrastructure, lower maintenance overhead, and streamlined cross-border data exchange. Member States benefit from significant cost efficiencies, including reduced investments in hardware, software licenses, maintenance and IT staffing, with indicative savings estimated at 15-30 % compared to independent deployments. Operationally, national authorities gain faster access to cross-border data, harmonised analytical outputs, and real-time collaboration capabilities, while reducing duplication of effort and inconsistencies between systems.

Over time, the enhanced processing capacity and secure digital architecture will enable faster analytics, improved operational coordination, and more automated workflows. These efficiencies allow both Europol and Member States to reallocate resources toward strategic and operational priorities, strengthening collective investigative capabilities while ensuring a scalable, secure, and future-proof digital backbone for EU internal security cooperation.

Sub policy option 2.4: Measure 2 on Europol support offices

Taking into account **standard EU employment costs**, including salaries, social security contributions, expatriation and household allowances where applicable, as well as limited operational expenditure such as secure IT connectivity, encrypted communications, basic office equipment and essential coordination travel, a modest Europol support office would be expected to generate **EU-level costs in the range of approximately EUR 400,000 to EUR 650,000 per year**. This estimate assumes a small footprint structure, composed of a limited number of specialised staff embedded in or co-located with relevant national counterparts, without requiring significant infrastructure investment.

Under a **limited rollout scenario of five to ten Europol support offices**, annual EU-level costs would therefore likely range between approximately **EUR 2 million and EUR 6.5 million**, corresponding to approximately EUR 14 million to EUR 45.5 million cumulatively over the 2028–2034 MFF period, depending on staffing levels, host-country conditions and the intensity of operational engagement. These estimates remain proportionate, as they reflect a light and scalable deployment model focused on coordination, facilitation and analytical support rather than autonomous operational structures. Over time, such offices could generate indirect efficiency gains by improving information flows, accelerating case coordination and reducing transaction costs linked to cross-border cooperation.

III. Contribution to the administrative burden reduction targets					
Administrative costs	***New recurrent costs (INs)***	***Removed recurrent costs (OUTs)***	***Net cost (Ins – OUTs)***	***New one-off costs (Ins)***	***Removed one-off costs (OUTs)***
All businesses	n/a	n/a	n/a	n/a	n/a
in which SMEs	n/a	n/a	n/a	n/a	n/a
Public administrations	n/a	n/a	n/a	n/a	n/a
Citizens	n/a	n/a	n/a	n/a	n/a

IV. Overview of relevant Sustainable Development Goals	
Sustainable Development Goals	***Expected progress towards the goal***
No. 16: Peace, justice, and strong institutions	The initiative is expected to strengthen the rule of law and enhance security within the EU by reinforcing the operational effectiveness of Europol. Clarifying and, where appropriate, reinforcing the role of Europol in supporting Member States in the fight against cross-border and serious organised crime will enhance the Agency's contribution to

	tackling transnational threats, including terrorism, cybercrime and other forms of serious crime, thereby supporting broader EU security objectives. Improved coordination, information exchange and operational cooperation among Member States, facilitated by Europol, are expected to lead to more effective law enforcement outcomes. This, in turn, may contribute to increased public trust in national authorities and EU institutions, particularly in the EU's capacity to address complex and evolving security challenges.

Benefits of the preferred option

The table below presents the overview of benefits for the preferred option.

I. Overview of Benefits (total for all provisions) – Preferred Option		
Description	***Amount***	***Comments (main recipients of the benefits)***
Direct benefits		
Strengthened data availability, processing and service.	The implementation of this policy options will lead to significantly reduced ad-hoc requests for information, as Member States gain access to more complete and structured datasets. This will enable faster access to relevant data for investigations and provide more reliable information for operational analysis and cross-border cases, improving both the quality and timeliness of investigative outputs. At EU level, these improvements will allow Europol to deliver better analytical outputs and more effectively support EU-wide operations, ensuring that law enforcement and judicial authorities across the Union can act on accurate, comprehensive, and actionable information.	National law enforcement authorities of the EU Member States, Europol.
Strengthened continuum of EU-level support to law enforcement cooperation through Europol and judicial cooperation through Eurojust.	By effectively exchanging relevant operational information, Europol and Eurojust will be able to better support national law enforcement and judicial authorities in line with their respective mandates (for instance, thanks to earlier detection of links between cases). For Europol, this includes the ability to produce a more complete EU-level criminal intelligence picture. National authorities of the EU will be able to rely in a stable and foreseeable long-term manner on specialised knowledge and expertise jointly provided by Europol and Eurojust to successfully obtain critical electronic evidence for criminal	National law enforcement and judicial authorities of the EU Member States, Europol, Eurojust, private parties.

	investigations and prosecutions, including in partnership with private parties	
Europol digital platforms embedded in national investigations.	Upgrading and integrating national and EU systems allows for more efficient queries, automated workflows, and standardised data processing. This reduces repetitive manual tasks and improves the speed and reliability of investigative outputs. Member States benefit from long-term operational savings, as integrated systems facilitate more effective searches, increased detection of relevant data and leads, and stronger cross-border investigations, reinforcing both national and EU-wide law enforcement capabilities.	National law enforcement authorities of the EU Member States, Europol.
Europol as an operational service provider and information hub	This option enhances Europol's ability to use available information effectively, providing dedicated forensic experts and operational staff to handle queries and analyse data. Member States benefit directly by reducing the need to perform time-consuming searches themselves, saving both personnel time and operational costs. At the EU level, the improved operational capacity ensures that cross-border and EU-wide investigations are supported with more accurate, timely, and actionable intelligence, reinforcing the overall law enforcement response and delivering tangible efficiency gains across the Union.	National law enforcement authorities of the EU Member States, Europol.
Simplified rules to reduce the administrative burden of data subject categorisation (DSC)	This option will reduce the administrative burden associated with the management of DSC procedures, lowering the personnel resources required to carry out labour-intensive administrative tasks. By simplifying these processes, it will allow both Member States and Europol to allocate staff time more efficiently to operational activities. At the same time, Europol will benefit from greater flexibility in the use of certain categories of data that were previously subject to stricter procedural limitations. This will increase the volume and operational relevance of information available for analysis, thereby strengthening Europol's analytical capabilities. Member States and Europol will therefore realise efficiency gains through reduced staff time devoted to DSC-related administrative procedures, while maintaining a robust legal framework. Alignment with the EUDPR and the LED, to the extent required to establish an appropriate framework for Europol, will ensure legal certainty and consistency with the EU data protection acquis. Overall, the streamlined approach will facilitate	National law enforcement authorities of the EU Member States, Europol.

	more efficient information handling and intelligence analysis, supporting cross-border investigations and enabling more effective information sharing between Member States and Europol.	
Europol as structural provider of information, analytical support and capacities to the EPPO	The financial interests of the EU will be protected as the EPPO will be able to fulfil its mission effectively (thanks to Europol's reinforced support) and efficiently (thanks to direct access to information stored by Europol and hierarchal arrangements between EPPO and Europol). For Europol, structural cooperation with the EPPO will lead to the ability to produce a more complete EU-level criminal intelligence picture and thus better support national law enforcement authorities.	EPPO, national law enforcement authorities of the EU Member States, Europol.
EU Digital Police Cloud	The EU Police Cloud provides scalable storage and processing power for law enforcement applications, generating economies of scale that prevent each Member State from investing individually in expensive digital infrastructure. This ensures faster, more secure and harmonised access to critical tools and datasets. Member States save resources and gain operational efficiency by leveraging shared infrastructure, while Europol benefits from centralised processing, enhanced analytical capacity, and support for EU-wide operations, delivering tangible long-term gains in both cost and effectiveness.	National law enforcement authorities of the EU Member States, Europol.
Europol support offices	By significantly improving the practical uptake of Europol's support (analytical, operational, and strategic products) by national authorities thanks to swifter, faster and more systematic access, this measure strengthens the effectiveness and efficiency of national investigations, as well as and the quality and timeliness of the EU-wide criminal intelligence picture provided by Europol.	National law enforcement authorities of the EU Member States, Europol.
Indirect benefits		
None identified		

The preferred option clearly identifies two areas where the direct benefits could result in substantial figures. Those are:

- Potential efficiency gains from joint procurement in EU internal security
- Potential gains due to the EU Police Cloud

Potential efficiency gains from joint procurement in EU internal security

According to Eurostat statistics on government expenditure by function, expenditure by EU Member States on public order and safety amounted to approximately **1.7% of EU GDP in 2023**[162]. This category includes expenditure related to police services, fire protection services, law courts, prisons and related research and development.

On the basis of the current size of the EU economy, this corresponds to approximately **€270–290 billion annually** across the Union. Within this category, **police services account for around 0.9% of EU GDP**, representing the largest component of public order and safety expenditure.

This spending supports a wide range of operational capabilities, including personnel, infrastructure, and operational equipment used by law enforcement authorities. In recent years, the technological component of law enforcement capabilities has increased significantly, reflecting the growing role of digital evidence, cyber investigations, use of biometric technology and data-driven policing in combating organised crime and terrorism.

Procurement of law enforcement equipment and technologies is largely carried out at national, and in some cases regional or local, level. As a result, procurement markets for law enforcement technologies in the Union are characterised by a high degree of fragmentation.

Fragmentation can lead to a number of inefficiencies, including:

- duplication of procurement procedures across Member States;
- reduced purchasing volumes for similar technologies;
- limited interoperability between equipment and systems used by different authorities;
- weaker bargaining power vis-à-vis suppliers.

These issues are particularly relevant in areas where technologies are widely used by law enforcement authorities across the Union, including digital investigation tools, forensic technologies and data-analysis capabilities.

Similar challenges related to fragmentation of procurement markets have been identified in the defence sector. In its analysis of defence capability development, the Commission has highlighted that fragmentation of procurement across Member States may lead to higher costs and reduced efficiency. In this context, the Commission has estimated that **joint procurement of defence equipment could generate savings of around 10% on the value of equipment procured jointly**, notably through economies of scale, stronger bargaining power, and reduced duplication of procurement processes[163].

---

[162] Eurostat (March 2025), *Government expenditure on public order and safety*, accessible at: Government expenditure on public order and safety - Statistics Explained - Eurostat

[163] SWD (2025) 820 final.

This analysis suggests that the aggregation of demand across Member States can generate efficiency gains in markets characterised by multiple national buyers and relatively concentrated supplier bases.

Although the operational contexts differ, procurement markets for certain law enforcement technologies display characteristics similar to those observed in the defence sector, including:

- a large number of public buyers across the Union;
- relatively limited numbers of specialised suppliers;
- increasing reliance on complex technological systems;
- the need for interoperability between national authorities.

These features are particularly visible in areas such as digital forensic tools, cyber-investigation technologies, biometric identification systems, case management systems, and data-analysis platforms used in criminal investigations.

In such areas, voluntary joint procurement mechanisms at Union level via Europol could allow participating Member States to aggregate demand for commonly used technologies. This could contribute to improved purchasing conditions, facilitate interoperability of systems used by law enforcement authorities and reduce duplication of procurement efforts.

While the magnitude of potential efficiency gains would depend on the scope and level of participation in joint procurement arrangements, experience from other sectors indicates that aggregation of demand may generate both financial and operational benefits.

Potential advantages include:

- **economies of scale**, resulting from larger procurement volumes;
- **improved bargaining power** vis-à-vis technology suppliers;
- **reduced administrative costs** associated with procurement procedures;
- **greater interoperability** of technological systems used by law enforcement authorities;
- **faster deployment of new capabilities** across Member States.

Such mechanisms could complement existing Union-level initiatives aimed at strengthening operational cooperation between law enforcement authorities, including those supported by Europol.

If we considered the above, by leveraging economies of scale, reducing duplicated administrative effort, and increasing bargaining power, joint procurement could achieve **conservative savings of 10%** compared to each Member State conducting procurement individually. For example, a total estimated cost of EUR 200 million across 20 Member States could be reduced to approximately EUR 180 million under a joint procurement approach. These savings reflect both lower unit prices and reduced administrative burdens, while maintaining compliance with EU procurement rules and ensuring harmonised quality standards.

Given the scale of public expenditure on public order and safety in the Union and the increasing importance of technological capabilities in law enforcement activities, the aggregation of demand through voluntary joint procurement mechanisms could contribute to improving the efficiency of public spending in this area.

Experience in other sectors, including defence, indicates that joint procurement may generate significant efficiency gains where procurement markets are fragmented and characterised by multiple public buyers. Similar mechanisms could therefore offer potential benefits in specific areas of law enforcement technology procurement, while also supporting greater interoperability and operational cooperation between Member States.

Potential gains due to the EU Police Cloud

In the absence of concrete figures, this section aims to explain the logic behind the potential gains due to the EU Police Cloud. The **EU Police Cloud** would provide scalable storage and processing capacity for law enforcement applications at Union level. By pooling digital infrastructure, it would generate **economies of scale** compared to multiple independent national deployments.

The volume of **digital evidence processed by law enforcement authorities is increasing rapidly**, driven by the growing use of online communications, encrypted messaging services, digital devices and data-intensive investigations. This trend requires expanded storage capacity and advanced computing capabilities to process large datasets, including for digital forensics, cybercrime investigations and data analytics. Shared infrastructure can address these growing needs more efficiently than multiple smaller national systems, enabling law enforcement authorities to access scalable and adaptable computing resources.

In the absence of a shared platform, Member States would need to invest individually in digital infrastructure, including data-storage systems, computing capacity, cybersecurity services and software licences, notably for EU classified infrastructure. A shared EU platform would lower the minimum cost of entry to highly specialized infrastructure and shared tools, avoid duplication of such investments and allow participating authorities to benefit from common infrastructure and services.

While the investment costs for cloud infrastructure itself are relatively limited compared with the broader operational costs of analytical capabilities, economies of scale can be achieved through several mechanisms. First, a shared platform would reduce duplication in data collection and processing, as the same datasets, including those obtained through open-source intelligence tools or specialised licences, would not need to be collected and analysed separately by multiple authorities. Second, computing resources could be allocated dynamically across participating users, allowing processing power to be distributed more efficiently depending on operational needs. This type of shared resource management can generate significant efficiency gains, with potential reductions in processing requirements estimated in the range of **50–70% compared with fragmented national deployments**.

In addition, the shared platform would significantly lower the cost of access to highly specialised capabilities, including infrastructure compliant with **EU RESTRICTED**

classification requirements and advanced analytical services. For many national authorities, developing such capacities individually would require substantial upfront investment and specialised expertise, which can be more efficiently provided through a common EU-level platform.

Member States could therefore reduce costs related to hardware procurement, software licensing, system maintenance and IT staffing, while gaining access to more advanced analytical capabilities than might be available through smaller national deployments. The use of a common infrastructure for public data, such as Child Sexual Abuse (CSA) material from the Internet or the dark web and joint investigative data will *a minima* halve the cost of storage and processing, as well as the cost of the collection of public data including from the dark web. The dedicated processing capacities (GPUs) made available by the EU Police Cloud would be allocated over more law enforcement authorities and more users, allowing a more efficient use of such capacities, by evening out over time the Member States instant peaks. Note that this economy of scale could not be reached at national level with other governmental authorities for sensitivity and confidentiality reasons.

Europol would also benefit from centralised processing capacity, facilitating the analysis of large datasets and supporting EU-wide operational activities.

Overall, the use of shared digital infrastructure could generate **significant efficiencies over time** by spreading infrastructure costs across multiple users and avoiding parallel investments by individual Member States.

3. RELEVANT SUSTAINABLE DEVELOPMENT GOALS

IV. Overview of relevant Sustainable Development Goals – Preferred Option(s)		
Relevant SDG	**Expected progress towards the Goal**	**Comments**
SDG 16 – peace, justice and strong institutions	Faster identification and joint analysis of cross-border criminal activities enable investigations to be carried out earlier and better, empowering effective responses by national law enforcement agencies and thus strengthening effective institutions and rule of law. Stronger cooperation between Europol and Eurojust as well as Europol and the EPPO will strengthen the EU-level fight against organised crime and thus the rule of law within the EU and its Member States, including better protecting the financial interest of the EU.	

ANNEX 4: ANALYTICAL METHODS

1. METHODOLOGICAL APPROACH

This Impact Assessment has been prepared by the Commission services in accordance with the Better Regulation Guidelines and Toolbox. The analytical framework structures the assessment of problems, objectives, policy options and impacts in a consistent and traceable manner. An external study supported the evidence base and analytical work.

The intervention logic links identified problems and their drivers to specific objectives and to the measures included under each policy option. Coherence is ensured between the evaluation findings (Annex 7), the problem definition in the main report, and the comparative assessment of impacts. Each option was assessed against a clearly defined baseline scenario reflecting the continuation of the current legal and operational framework. The baseline scenario reflects the continuation of the current legal mandate, governance structure and operational model, including already programmed developments. It does not assume structural mandate changes beyond the current framework. This counterfactual ensures that impacts attributed to the initiative represent incremental effects compared to the *status quo*.

Three core assessment criteria guided the analysis:

- **Effectiveness**: the extent to which the option is expected to achieve the initiative's objectives.
- **Efficiency**: the relationship between the resources required and the results expected, including distributional effects.
- **Coherence**: the internal consistency of the option and its alignment with other relevant EU legislation and policy objectives.

The analysis also considers **proportionality** and EU added value.

1.1 Methodology for assessment of impacts

Effectiveness

Effectiveness was assessed by examining the extent to which each policy option addresses the identified problems and contributes to the initiative's specific and general objectives. The analysis draws on evaluation findings, operational data, stakeholder feedback and expert judgement. Where available, quantitative indicators informed the assessment. In areas where quantitative indicators were not available, structured qualitative analysis was applied.

The assessment considers not only formal legal changes but also implementation feasibility and operational practicality.

Efficiency

Efficiency was evaluated by analysing the proportionality between expected benefits and the resources required under each policy option. The analysis covers:

- Financial costs at EU level;
- Implementation efforts at EU and national level where relevant;
- Administrative burden and compliance implications;
- Social impacts and potential effects on fundamental rights;
- Distribution of costs and benefits across stakeholders.

Costs and benefits were assessed both in quantitative and qualitative terms. Where monetisation was not feasible, impacts were characterised in terms of expected magnitude and operational significance. The analysis explicitly distinguishes between one-off implementation costs and recurring operational costs.

The proportionality principle guided the assessment: resource implications were evaluated against expected operational improvements, including enhanced coordination, strengthened analytical capacity, improved information exchange and reduction of fragmentation.

Coherence

Coherence was examined by assessing the consistency of each option with related EU legislation, in particular the ProtectEU Strategy, existing institutional mandates and broader policy objectives. The analysis identifies potential overlaps, complementarities or tensions with other instruments at EU and national level.

2. COSTING METHODOLOGIES

The costing exercise provides indicative *ex ante* estimates of the financial and operational implications of the policy options. Given the varying degree of specification of measures and differences in data availability, a mixed-method approach combining quantitative and qualitative evidence was applied.

Quantification was undertaken only where sufficiently reliable and granular data were available. Where implementation parameters remain dependent on future operational or technical decisions, impacts were assessed qualitatively in order to avoid artificial quantification.

2.1 Evidence base for quantification

Quantitative analysis relied primarily on Europol's annual budget, establishment plans and Single Programming Documents. These sources enabled:

- estimation of unit costs per full-time equivalent (FTE);
- allocation of costs between operational and enabling functions;
- modelling of scaling effects for analytical, operational and compliance capacities;
- differentiation between capital expenditure and recurring expenditure.

For selected measures involving regulatory and compliance functions, quantitative inputs were drawn from Commission Staff Working Documents and administrative reporting, including cost modelling related to temporary data processing under Article 18 of the Europol Regulation and reporting to the Joint Parliamentary Scrutiny Group.

Publicly available remuneration benchmarks were used, where relevant, to estimate staffing costs for potential new organisational structures.

2.2 Benchmarking and modelling

Where direct measurement was not feasible, project-level financial data from comparable EU-level initiatives were used as benchmarks. These include platforms such as the SIRIUS project and the Joint Operational Analysis Case (JOAC) platform. These benchmarks provided reference points for development costs, staffing structures and operational expenditure.

For infrastructure-intensive or digital measures, including the EU Digital Police Cloud, scenario-based modelling was applied over a multi-annual horizon. Financial projections incorporated known technical constraints, including projected data volume growth, system performance requirements, data-centre capacity limits, and expected system usage intensity.

Alternative scenarios reflected varying levels of technical ambition and investment scale. Costs were systematically differentiated between one-off implementation expenditure and recurring adjustment costs related to maintenance, licences, managed services and ongoing support.

2.3 Human resources

Human resource impacts were explicitly quantified where measures implied structural expansion of analytical, operational or compliance functions. Quantification relied on activity-based costing, operational workload benchmarks and scenario-based scaling of staffing needs.

Where quantitative operational data were insufficient to support monetisation, staffing impacts were assessed qualitatively and characterised conservatively.

2.4 ICT and interoperability

ICT-related costs were identified for measures that explicitly require IT infrastructure, system development or integration, data-processing platforms, large-scale information exchange mechanisms, or a material expansion of Europol's digital and analytical environment. For a substantial share of measures, ICT impacts were assessed as negligible or limited, on the assumption that they build on existing Europol systems, interoperability frameworks and national infrastructures without requiring major upgrades. The quantification and qualitative assessment of ICT costs followed three approaches depending on the nature of the measure and data availability: incremental adjustment of existing systems; proportional scaling of enabling ICT capacity alongside operational expansion; and scenario-based modelling for large digital platforms and collaborative environments.

The latter approach was applied in particular to the EU Police Cloud. In these cases, financial projections were developed over a multi-annual period, incorporating known technical constraints such as projected data volume growth, existing data-centre capacity limits, legal restrictions affecting outsourcing, and the scale and duration of large ICT programmes. Alternative scenarios were used to reflect varying levels of investment ambition and technical capability, ranging from limited system upgrades to more advanced configurations involving cloud solutions, enhanced security features, automation and advanced analytics. ICT costs were therefore differentiated between one-off

implementation costs and recurring adjustment costs related to maintenance, licences, managed services and ongoing support.

For measures involving data exchange with other EU agencies, ICT costs are primarily driven by interoperability requirements and workload-dependent demand. In these cases, the analysis assumes that core systems are already in place and that additional costs mainly relate to integration, logging and auditing configurations, capacity management and maintenance. Benchmarks from comparable projects were used where relevant to approximate development and operating costs, with low and high-bound estimates applied to reflect uncertainty regarding future data volumes, query intensity and participation levels.

2.5 Infrastructure

Infrastructure costs include premises, secure facilities, equipment and organisational support services required to accommodate operational expansion. As such costs are highly dependent on future implementation choices and location-specific factors, they could not be estimated *ex ante* with sufficient reliability and were therefore not monetised. Their potential impact is described qualitatively.

3. CAVEATS AND LIMITATIONS

Uncertainty in cost projections was addressed through scenario analysis and the use of lower- and upper-bound estimates where appropriate. Key variables subject to sensitivity considerations include staffing levels, data volumes, ICT scaling requirements and participation rates.

Where impacts could not be reliably monetised, qualitative assessment was applied. Conservative assumptions were used in order to avoid overstating benefits or underestimating costs.

Certain limitations are inherent to *ex ante* assessments of complex institutional reforms. Some implementation parameters depend on future operational decisions, legislative negotiations or technological developments. In such cases, impacts are presented proportionately and transparently, ensuring analytical robustness without over-precision.

Despite these limitations, the consistent comparative framework applied across policy options ensures that the relative differences between options are analytically sound and that conclusions are evidence-based and proportionate.

ANNEX 5: THE PREFERRED POLICY MEASURES

The combined effect operates along three mutually dependent pillars: **data availability, legal usability and technical-operational capacity**. The contribution of each measure to the operational objectives will be reported under the section on the preferred policy option.

Legal enabler: Data Subject Categorisation

The reform of Data Subject Categorisation (DSC) of policy option 2.2 constitutes a **horizontal enabler** for the entire package. By streamlining and aligning the DSC framework, it removes structural constraints affecting the timely processing of large and complex datasets.

This directly strengthens the effectiveness of:

- **Sub policy option 1.1**, by facilitating faster and more consistent data uploads;
- **Sub policy option 2.1**, by enabling more efficient cross-border exploitation of shared data;
- **Sub policy option 1.4**, by ensuring that systematic consultation mechanisms function without procedural bottlenecks;
- **Sub policy option 2.4**, by providing legal clarity for scalable cloud-based analytics.

Data availability and systematic use

Options 1.1 and 2.1 improve the **quantity, quality and cross-border use of data**, within proportionate limits. Automated data loaders and structured workflows ensure more consistent contributions from Member States. Option 1.4 embeds Europol systems into national workflows and makes cross-border checks systematic.

More information at Europol strengthens the EU intelligence picture and directly enhances cooperation with EPPO and Eurojust. Conversely, structured data inflows from EPPO, Eurojust and other EU actors increase the analytical value of Europol datasets by enabling broader cross-checks and correlation.

Together, these measures will contribute to the operational objectives of:

- Improving information exchange by increasing the volume and reliability of operational data at EU level and reducing fragmentation and uneven participation;
- Reducing delays and increasing actionable intelligence by ensuring that shared data is systematically queried and exploited.

Structural enablers

Sub policy options 1.3 and 2.3 **reinforce the institutional architecture** at EU level:

- Institutionalisation of SIRIUS ensures sustainable support to national authorities in accessing electronic evidence.

- Upgrading and automating the Europol–Eurojust hit/no-hit mechanism, and extending indirect access, enhances structured inter-agency information exchange.
- A reinforced partnership with the EPPO, including a dedicated team at Europol, ensures predictable, specialised and high-quality analytical support.

Processing capacity and scalability

The EU Police Cloud (Sub policy option 2.4) provides the **scalable infrastructure necessary to absorb and analyse increased data flows**. It enables secure storage, advanced analytics and structured collaboration at scale. Enhanced analytical tools (including those under Sub policy options 1.1, 1.3 and 2.1) and strengthened Europol–EPPO cooperation (Sub policy option 2.3) ensure that increased data volumes translate into operational results rather than administrative burden.

The combined dynamic is cumulative: More structured data → improved analytics → stronger operational insights → more effective cross-border cooperation.

Financial coherence and cost synergies

Certain investments under Sub policy options 1.1 and 1.4 **overlap**, particularly in relation to system upgrades and integration components. Implemented together, these elements avoid duplication, meaning that the combined investment remains broadly aligned with the previously estimated envelope (approximately **EUR 30 million** in system modernisation), rather than accumulating mechanically.

Economies of scale, reduced duplication and structured EU-level coordination further enhance cost-efficiency.

Overall assessment

Taken together, the preferred options form a **coherent, cumulative and scalable reform package**:

- **Sub policy option 2.2 removes legal bottlenecks;**
- **Sub policy options 1.1 and 2.1 increase data availability and cross-border use;**
- **Sub policy option 1.3 strengthens inter-agency cooperation and information exchange;**
- **Sub policy option 2.3 anchors Europol as a structural analytical partner of the EPPO;**
- **Sub policy option 1.4 ensures systematic operational embedding;**
- **Sub policy option 2.4 provides the digital backbone and scalability.**

Their combined implementation directly supports the operational objectives identified in this Impact Assessment and will be subject to structured monitoring and evaluation to ensure measurable improvements in information exchange, analytical capacity and cross-border operational effectiveness.

The package therefore delivers a proportionate and mutually reinforcing response to the evolving digital and transnational nature of serious and organised crime.

The preferred package combines **Sub policy options 1.1 + 2.1 (limited to Prüm II and without broader interoperability), Sub policy option 2.2 (Data Subject Categorisation reform), Sub policy option 1.3 (enhanced EU inter-agency cooperation limited to Eurojust), Sub policy option 2.3 (structural Europol–EPPO partnership) and Sub policy options 1.4 + 2.4 (structural integration and EU Police Cloud)**. Together, these measures form a coherent and mutually reinforcing reform of the EU law enforcement information architecture.

	Preferred policy option 1.1 + 1.3 + 1.4 + 2.1+ 2.2 +2.3+ 2.4
assessment criteria	
1) Impact on citizens	++
2) Impact on national authorities	++
3) Objective of general interest	++
4) Data protection	0
5) Costs	+
6) Feasibility	+
7) Impact on digitalisation	++

a. Impact on citizens (++)

Each of the preferred options individually contributes to strengthening EU internal security; combined, their impact is **cumulative and mutually reinforcing**. By improving the availability, quality and usability of data (1.1, 1.4, 2.1, 2.2), enhancing structured inter-agency and prosecutorial cooperation (1.3, 2.3), and providing scalable digital and analytical capacity (2.4), the package directly addresses the three core problems identified: persistent information gaps in cross-border investigations, fragmented and uneven operational coordination, and structural resource and capability constraints at EU level.

In practical terms, this translates into **earlier detection of criminal networks, faster identification of cross-border links, improved asset tracing, and more coordinated operational action across Member States**. Strengthened analytical capabilities and streamlined information flows reduce delays, minimise duplication of efforts and increase the likelihood that criminal activities are detected before harm escalates. At the same time, reinforced cooperation with EU partners and prosecutorial authorities supports stronger case-building and higher-quality evidence, contributing to more effective prosecutions.

Overall, the combined measures significantly enhance the capacity of Europol and national authorities to **prevent, investigate and disrupt serious and organised crime**, including

in the digital domain, thereby delivering a **substantially higher level of protection for citizens** in both physical and online environments, while operating within a robust framework of data protection and fundamental rights safeguards.

b. Impact on national authorities (++)

Each of the preferred options individually strengthens national authorities' operational capacities; taken together, their impact is **systemic and mutually reinforcing**. By closing information gaps and improving structured data exchange (1.1, 1.4, 2.1, 2.2), reinforcing EU-level coordination and prosecutorial cooperation (1.3, 2.3), and providing scalable digital infrastructure and advanced analytical tools (2.4), the package directly tackles fragmented cross-border information flows, uneven coordination and structural constraints in resources and technical capabilities.

In practical terms, national authorities benefit from **faster access to relevant intelligence, improved cross-border link detection, stronger analytical support and more predictable cooperation channels**. Streamlined procedures and clearer frameworks enhance legal certainty and reduce operational friction, while shared digital tools and specialised expertise help address capacity gaps, particularly in complex areas such as cybercrime, financial investigations and large datasets. Overall, the measures reinforce Member States' ability to **act effectively, cooperate efficiently and rely on sustained EU-level support**, strengthening both day-to-day operational performance and long-term resilience against increasingly sophisticated and digitalised criminal threats.

c. Impact on fundamental rights

Objective of general interest (++)

Each of the preferred options contributes individually to strengthening the Union's **Area of Freedom, Security and Justice**; combined, they create a **more coherent, resilient and future-proof internal security framework**. By reinforcing structured information exchange, operational coordination and digital capabilities, the package enhances the Union's collective capacity to prevent and combat serious and organised crime in an increasingly cross-border and digitalised threat environment.

The measures also strengthen **mutual trust and solidarity among Member States**, ensure more effective interaction between EU bodies, notably Europol, the EPPO and Eurojust and reduce fragmentation in the EU security architecture. By investing in shared digital and analytical capacities, the Union advances its **strategic autonomy in law enforcement technologies and expertise**, reducing reliance on external tools while maintaining high standards. Overall, the initiative supports the objective of delivering a **high level of security across the EU**, firmly anchored in respect for fundamental rights, data protection and the rule of law.

Impact on data protection (0)

The impact of the preferred package on data protection is considered overall **neutral**, as all retained options have successfully passed both the **necessity** and **proportionality** assessments.

Necessity. The measures respond to clearly identified structural problems, persistent information gaps, fragmented cross-border exchanges and inefficiencies in data handling, which cannot be effectively addressed by Member States acting alone. The initiative does not introduce new categories of personal data nor expand the purposes of processing. Instead, it seeks to improve the relevance, structure and operational usability of data already lawfully processed within the existing legal framework. By optimising information flows and clarifying procedural conditions, the package ensures that processing remains strictly linked to operational needs in combating serious and organised crime.

Proportionality. The preferred options are limited to what is necessary to achieve the identified objectives and avoid excessive or unjustified data processing. They build on existing systems and legal bases, refrain from creating parallel databases or duplicative storage, and maintain decentralised responsibilities where appropriate. Safeguards relating to purpose limitation, access control, oversight and data subject rights remain fully applicable. Particular attention has been paid to ensuring that enhanced analytical capacities and improved interoperability do not alter the balance between operational effectiveness and fundamental rights protection.

The reform of **Data Subject Categorisation (Option 2.2)** simplifies an existing safeguard to remove structural inefficiencies and reduce administrative burden, while maintaining the core protective logic of differentiated data handling. This adjustment strengthens legal clarity and aligns more closely with the framework of the EUDPR and the Law Enforcement Directive, without lowering the level of protection.

Overall, the combined measures preserve a **high level of data protection**, while enhancing coherence, transparency and accountability in EU law enforcement information processing.

e) **Cost (+)**

	Member States	***Europol***
Direct costs		
Expected one-off costs (in million EUR) - *Policy option 1.1* - *Policy option 1.3* - *Policy option 1.4* - *Policy option 2.1* - *Policy option 2.2* - *Policy option 2.3* - *Policy option 2.4*	***254.85*** - *81* - *0* - *105* - *1.35* - *0* - *0* - *67.5*	***267.3*** - *61** - *2* - *50** - *11* - *0* - *0* - *143.3*
Expected yearly recurring costs (in million EUR) - *Policy option 1.1* - *Policy option 1.3* - *Policy option 1.4* - *Policy option 2.1*	***47.9*** - *16.2* - *0* - *20* - *0.3*	***77.3*** - *12.2* - *1* - *8* - *5.3*

- *Policy option 2.2* - *Policy option 2.3* - *Policy option 2.4*	- *0* - *0* - *11.4*	- *0* - *11* - *39.8*

The combined package entails **cumulative investments** at both Member State and EU level, while generating important efficiencies through synergies and rationalised implementation. In particular, overlaps between Policy Options 1.1 (strengthening information exchange) and 1.4 (CMS integration and workflow embedding) create **economies of scale** estimated at approximately EUR 30 million, reducing overall expenditure compared to a purely additive approach.

The **one-off costs** reflect initial investments in system upgrades, deployment of technical infrastructure, training, and integration of digital and analytical tools. For Member States, these are estimated at EUR 254.85 million, while for Europol they amount to EUR 237.3 million. **Recurring annual costs** cover ongoing maintenance, operational support, staffing, and continuous improvements to systems and services, amounting to EUR 47.9 million for Member States and EUR 77.3 million for Europol.

These figures represent a **consolidated and optimised implementation** of the preferred options, ensuring that operational impact is maximised while financial burdens are contained. Importantly, the investments are expected to generate **significant efficiency gains**: improved interoperability, automation of data flows, and enhanced analytical capacity will reduce time and resources needed for cross-border investigations. Over time, these operational efficiencies are likely to offset a portion of the recurring costs, while also increasing the overall return on investment in terms of faster investigations, better intelligence, and improved EU internal security outcomes.

Overall, the cost estimates demonstrate that the package is financially feasible, proportionate, and justified by the expected operational and strategic benefits for both Member States and Europol.

f) **Feasibility (+)**

All preferred options are individually **technically feasible**, as they build on existing legal frameworks, operational practices, and IT infrastructures at both EU and national level. When combined, they form a **reinforced and coherent technical package**: increased data availability and streamlined categorisation (1.1, 2.1, 2.2, 1.4) feed directly into strengthened inter-agency and prosecutorial cooperation (1.3, 2.3), while the EU Police Cloud (2.4) provides the **scalable digital infrastructure** necessary to support expanded analytical use, advanced data matching, and secure cross-border workflows. The approach relies primarily on **upgrading and integrating existing systems**, rather than creating entirely new architectures, ensuring continuity, manageability, and reduced implementation risk. Synergies with established EU technological frameworks, including those developed by **eu-LISA**, further enhance feasibility by leveraging proven interoperability standards, secure authentication mechanisms, and shared infrastructure components. Collectively, these measures generate **cumulative efficiencies**, enabling the package to deliver greater operational impact than the sum of individual options.

From a **political feasibility** perspective, each option is achievable when considered individually, as all are anchored in existing cooperation frameworks and respect the division of competences between the Union and Member States. Certain elements, notably strengthened EU-level coordination, DSC reform and the structural reinforcement of Europol's role vis-à-vis the EPPO, may encounter reservations from stakeholders traditionally cautious about deeper integration. However, the package remains proportionate and firmly rooted in **operational needs identified by Member States themselves**, and its design emphasizes **support rather than substitution** of national responsibilities. Taken together, the measures form a **balanced and pragmatic reform**: they enhance EU-level support, strengthen operational effectiveness and provide scalable and resilient tools while preserving Member State decision-making and oversight.

By improving the efficiency and coherence of cross-border investigations, enabling better use of shared intelligence, and embedding upgraded technical infrastructure, the combined package is **technically achievable, politically realistic, and institutionally well grounded**. It ensures high data protection standards, maintains Member State control over operational decisions, and creates a sustainable foundation for **future-proof EU internal security cooperation**.

g) **Impact on digitalisation (++)**

All preferred options with a digital dimension have a **positive impact on the digital transformation of EU law enforcement cooperation**, as they modernise data exchange, streamline digital processing frameworks, and strengthen analytical and cloud-based capacities. By improving the automation, standardisation, and interoperability of existing systems, these options reduce manual workflows, accelerate the timeliness of cross-border intelligence sharing, and enhance the reliability and usability of operational data. Combined, their effect is **mutually reinforcing**: improved data availability and harmonised rules feed directly into stronger inter-agency and prosecutorial cooperation, while the EU Police Cloud provides a **scalable, secure and resilient digital backbone** capable of supporting advanced analytics, AI-assisted processing and structured cross-border workflows. In addition, the integration of national Case Management Systems with EU-level platforms further embeds digital tools into everyday investigative processes, ensuring that information flows efficiently and systematically without creating new access rights or duplicating datasets. Together, the package accelerates a **coherent and future-proof digitalisation** of EU internal security, enhancing operational effectiveness, fostering standardised digital practices across Member States, and creating a sustainable foundation for next-generation law enforcement capabilities.

ANNEX 6: MONITORING AND EVALUATION FRAMEWORK FOR THE PREFERRED POLICY MEASURES

Putting in place a structured framework for monitoring and evaluation will help ensure that the strengthened mandate under the preferred policy option translates into measurable operational, strategic and systemic benefits. The framework will establish clear links between the general and specific objectives, operational outputs, expected outcomes and broader impacts, supported by measurable indicators and, where feasible, baselines and targets. Monitoring arrangements will build on the mechanisms already established under Article 68 of the Europol Regulation, which foresees periodic evaluations of Europol's impact, effectiveness and efficiency. These mechanisms will be complemented by a refined indicator framework aligned with the specific and operational objectives of the preferred option.

Monitoring will focus on outputs (e.g. volume and quality of information exchange, operational support delivered), results (e.g. improved cross-border linkages identified, investigative acceleration), and broader impacts (e.g. strengthened EU-level situational awareness, reduced fragmentation in operational coordination). The framework will distinguish more clearly between outputs (activities and services delivered), outcomes (changes in operational cooperation and investigative effectiveness) and impacts (contribution to EU internal security objectives). Attention will be given to monitoring data-protection compliance, proportionality and fundamental rights safeguards, especially in relation to large and complex datasets and advanced analytical tools.

Core indicators will be drawn from a range of sources, including Europol's existing reporting instruments, including the Consolidated Annual Activity Report (CAAR); Article 7(11) reporting on Member State information contributions; EDPS supervisory findings and data protection reporting; SIENA Annual Reports; EIS Annual Reports; and Management Board performance indicators. Where possible, indicators will include baseline values and measurable targets to support the assessment of progress over time.

The Commission will monitor implementation through its representation on the Management Board, structured exchanges with Member States and Europol, and consultation with oversight bodies, including the EDPS. Data will also be drawn from SOCTA cycles, EMPACT performance reporting and, where appropriate, targeted stakeholder surveys.

Monitoring will begin from the entry into force of the revised Regulation. Indicators will be collected annually. A structured evaluation should be undertaken four years after entry into force, allowing sufficient time for operational maturation while ensuring that findings can inform any future legislative revision. The evaluation will assess effectiveness, efficiency, coherence, relevance and EU added value, including the extent to which the initiative has achieved the specific objectives and contributed to the overall objective. Where relevant, interim reviews may assess implementation bottlenecks, including technical interoperability and data-protection compliance burdens, in line with REFIT principles.

The monitoring framework below summarises the operational objectives and associated indicators per specific objective. It also identifies the corresponding outputs, outcomes and expected impacts to facilitate the assessment of operational success over time.

Specific objective	Operational objective	Indicator description	Data source	Targets / frequency
SO1: Reinforce Europol's role as an information hub	Strengthen Europol's capacity to collect, process, analyse and exchange criminal intelligence with Member States and improve the timeliness, interoperability and usability of information exchanges	• % of Member States technically integrated with Europol data-ingestion tools • % of operational data flows transmitted through automated channels • Average time between receipt of information by Europol and dissemination of operational leads • % of Europol-supported investigations relying on data from at least two Member States • Number of cross-system matches generating operational follow-up • Satisfaction score from Member States regarding Europol analytical support	SIENA and EIS transaction logs; CAAR; Article 7(11) reporting; Europol operational workflow logs; Europol user surveys	Annual monitoring; target increases to be defined in Programming Documents and Management Board KPIs
SO2: Strengthening Europol's capacity to support law enforcement operational action	Optimally integrate human resources between Europol and Member States	• Number of operational deployments and embedded Europol support arrangements • Average time-to-deployment following Member State request	Europol HR and deployment records; ENU coordination records;	Annual monitoring; deployment and training targets to be reviewed every two years

		• Number of specialised experts deployed in operational cases • Number of national officers trained in specialised investigative fields • Share of priority cases supported by specialised expertise	operational support office reporting	
	Ensure direct and proactive operational support by Europol to Member States and EPPO investigations	• Number and share of cross-border investigations supported operationally by Europol • Number and share of EMPACT and EPPO cases receiving Europol support • Number of proactive support offers initiated by Europol and accepted by Member States/EPPO • Share of cases where Europol support contributed to operational outcomes • Feedback score from	CAAR; operational reporting; EMPACT reporting; EPPO cooperation reporting; targeted stakeholder surveys	Annual monitoring with mid-term review after four years

		Member States and EPPO on operational usefulness		
	Enhance coordination and complementarity between Europol and relevant EU entities to reinforce synergies and ensure efficient resource use	• Number of joint operational activities with Eurojust, EPPO and other EU entities • Number of SIRIUS requests handled and median response time • Share of Europol-supported cases involving coordinated cooperation channels with Eurojust or EPPO • Number of structured information exchanges through hit/no-hit systems	Joint operational activity registers; SIRIUS platform metrics; cooperation logs; case-management systems	Annual monitoring; operational coordination targets to be reviewed in evaluation cycle

ANNEX 7: EVALUATION OF THE EXISTING POLICY AND LEGISLATIVE FRAMEWORK

1. Introduction

1.1. Purpose and scope

This evaluation assesses the performance of Regulation (EU) 2016/794, as amended by Regulation (EU) 2022/991, establishing the legal framework governing the European Union Agency for Law Enforcement Cooperation (Europol).

The evaluation is conducted in line with the **European Commission's Better Regulation Guidelines** and applies the standard evaluation criteria of **effectiveness, efficiency, relevance, coherence, and EU added value**. In this context, the analysis examines the extent to which the intervention has achieved its intended objectives, whether it has done so in a proportionate and resource-efficient manner, and whether the underlying policy rationale remains valid in light of the evolving security landscape in the European Union.

The evaluation covers the period **2017-2024**, corresponding to the implementation of Regulation (EU) 2016/794 and the initial application of the amendments introduced by Regulation (EU) 2022/991. The analysis therefore assesses both the functioning of the original regulatory framework and the initial impacts of the 2022 legislative changes.

The scope of the evaluation focuses on Europol's core tasks as defined in the Regulation, in particular its role in facilitating information exchange, providing criminal intelligence analysis, supporting operational coordination between Member States, developing specialised expertise through dedicated operational centres, and cooperating with EU institutions, agencies, third countries, and private actors. Particular attention is given to the extent to which the Regulation has enabled Europol to respond to the increasingly transnational, digitalised, and technologically sophisticated nature of serious crime and terrorism.

In addition to assessing operational performance, the evaluation examines whether the current legal framework provides Europol with the necessary tools to address emerging challenges. These include the increasing volume and complexity of data relevant to criminal investigations, and the need for law enforcement authorities to develop advanced technological capabilities, including in the areas of digital forensics, and data analytics. The analysis therefore considers whether the Regulation remains adequate to support Europol's evolving role within the EU's internal security architecture.

The evaluation also takes into account the broader policy context in which Europol operates, including the EU's internal security strategies and operational cooperation frameworks, such as the **ProtectEU Internal Security Strategy**. These policy initiatives shape Europol's operational priorities and provide an important reference point for assessing the continued relevance of the existing regulatory framework.

The findings of the evaluation contribute to the accompanying **impact assessment**, which examines potential policy options for revising Europol's mandate. The evaluation therefore provides the analytical basis for identifying possible shortcomings in the current legislative

framework and for assessing whether further policy or legislative action at EU level may be necessary.

1.2. Methodology

The evaluation draws on a **broad range of qualitative and quantitative evidence sources** in order to ensure a comprehensive assessment of the functioning of Regulation (EU) 2016/794, as amended by Regulation (EU) 2022/991.

The main evidence base for the evaluation was generated through an external study commissioned by the European Commission. The study supported the analytical work underpinning the evaluation, including evidence collection, stakeholder consultations, data analysis and the development of thematic case studies.

The external study supporting this evaluation was carried out by ICF S.A under Framework Contract 330302019 between July 2025 and March 2026.

The external study included extensive stakeholder consultations, public surveys and targeted interviews with relevant stakeholders. These consultations involved law enforcement officials from Member States, Europol officers directly involved in operational activities, and representatives of relevant EU institutions and agencies. The purpose of these consultations was to gather practical insights into how the Regulation functions in practice, including operational experiences, perceived added value of Europol's support, and potential challenges related to the implementation of the legal framework.

In total, 135 stakeholder interviews were held, including 12 explanatory interviews followed by 123 targeted interviews. They were conducted with national authorities of the EU Member States, including Denmark (56), Europol staff managers including managers and senior managers (35), European Commission services (14), EU agencies (8), EU bodies and offices (4), law enforcement networks (6), MAOC-N, third countries (5), international organisations (1), the private sector (2) and youth organisations (1).

The external study also included thematic case studies illustrating Europol's role in supporting specific operational activities and investigations. These case studies provide qualitative insight into how Europol's analytical capabilities, coordination functions and operational support contribute to concrete law enforcement outcomes at EU level. Field visits to Europol and five Member States[164], which also included further interviews, were conducted in order to gather qualitative and context specific evidence on Europol's cooperation with Member States.

In addition to the evidence generated through the external study, **the Commission carried out complementary evidence-gathering activities** in order to further inform the evaluation. These included **thematic workshops with relevant stakeholders**, which provided an opportunity to discuss specific operational and policy issues related to Europol's mandate and its future development.

The first two workshops were held on 6 and 7 November 2025, focusing on optimising Europol's data ecosystem and reinforcing its role as the EU's central operational hub and developing EU-level specialised law enforcement expertise and operational innovation

[164] Austria, Italy, The Netherlands, Slovenia, Sweden.

within Europol and reinforcing Europol's role in tackling persistent and emerging threats including within the EMPACT framework respectively. The third and fourth thematic expert workshops were held on 18 and 19 December 2025, with a focus on enhancing coordination and complementarily between Europol and relevant EU entities to reinforce synergies, ensure efficient resource use, and consolidate Europol's central role in the EU internal security infrastructure for the third workshop and on strengthening the steering and oversights of Europol to ensure effective governance in line with its growing operational tasks, budget and staff, while optimally integrating human resources between Europol and Member States for the fourth workshop.

Furthermore, **the Commission conducted targeted bilateral outreach to Member States' authorities, as well as exchanges with institutional stakeholders**, including the Council, in the context of COSI and the Law Enforcement Working Party, and the European Parliament, including the Joint Parliamentary Scrutiny Group. These exchanges helped gather additional perspectives on the implementation of the Europol Regulation, the practical functioning of Europol's mandate, and possible areas where the current legislative framework could be further strengthened.[165]

The evaluation also relies on **quantitative data analysis**, including operational statistics and performance indicators relating to Europol's activities and the use of its information systems and operational support tools. This analysis includes trend analysis of relevant indicators over the evaluation period in order to identify developments in Europol's operational role and the use of its services by Member States. Data sources used predominantly include Europol Annual Reports, SIENA statistics and annual reports, EIS annual reports, operational support statistics, Europol's annual budget, establishment plans and Single Programming Documents.

The combination of these sources enables the triangulation of evidence, allowing findings to be validated across multiple data sources and perspectives. Quantitative operational data are therefore assessed alongside stakeholder input and qualitative operational examples in order to identify both measurable outcomes and structural challenges in the implementation of the Regulation.

Nevertheless, **certain methodological limitations** should be taken into account when interpreting the findings of this evaluation. First, the availability and comparability of operational data across the evaluation period may be affected by changes in reporting practices, evolving performance indicators, and the progressive development of Europol's operational tools and systems. As a result, some trend analyses rely on partially comparable datasets or proxy indicators.

Second, evidence collected through stakeholder consultations and interviews reflects the perspectives of participating stakeholders and may therefore be subject to response bias or differences in national operational practices. While efforts were made to ensure balanced representation across Member States and stakeholder groups, the consultation results cannot be considered fully statistically representative of all users of Europol's services.

Third, given the evolving nature of criminal threats and technological developments, it is not always possible to attribute observed outcomes solely to the intervention. Europol operates within a broader and constantly evolving security

[165] More detailed information can be found in Annex 2 of the Staff Working Document.

environment shaped by multiple external factors, including developments in criminal activity, technological change, and variations in national law enforcement capacities. These external developments may influence observed outcomes, making it difficult in some cases to isolate the specific effects of the Regulation from broader contextual trends.

Where such limitations arise, the evaluation relies on the triangulation of multiple evidence sources in order to ensure that conclusions remain proportionate and robust. Further methodological details are provided in Annex 4.

2. What was the expected outcome of the intervention

2.1. Description of the intervention and its objective

Europol was founded under the **1995 Europol Convention** as a European Police Office to facilitate cooperation among national law enforcement authorities in combating serious cross-border crime. The Convention came into force 1 October 1998 and Europol became fully operational 1 July 1999. Initially, Europol focused on supporting information exchange between Member States through national contact points, analysing criminal intelligence, supporting investigations into organised criminal networks and maintaining centralised data systems. From its inception, Europol was designed to act as a hub for criminal intelligence sharing among Member States in order to address transnational crime phenomena such as terrorism, drug trafficking, trafficking in human beings, cybercrime and other forms of serious organised crime.

The Agency's legal framework evolved significantly with the Council Decision of 6 April 2009, which broadened Europol's operational scope and clarified its objectives, competences and tasks. The Decision removed the requirement to identify organised crime groups before action could be taken and expanded Europol's responsibilities to additional crime areas, including money laundering, trafficking in human beings, trafficking of cultural goods, racism and xenophobia and environmental crime. It also strengthened Europol's operational role by enabling it to request the initiation of investigations, support Joint Investigation Teams (JITs) and produce strategic threat assessments.

Council Framework Decision of 13 June 2002 established the legal framework for Joint Investigation Teams to facilitate cross-border investigations and judicial cooperation. The 2009 Council Decision subsequently authorised Europol staff to participate in JITs, allowing the Agency to support investigations directly within its mandate.

Regulation (EU) 2016/794 replaced the 2009 Council Decision and strengthened Europol's legal framework as the EU agency for law enforcement cooperation. The Regulation introduced enhanced governance and accountability mechanisms, including scrutiny by the European Parliament and national parliaments, as well as supervision of Europol's data processing activities by the European Data Protection Supervisor (EDPS). It also clarified and expanded Europol's mandate and established the legal basis for specialised centres within Europol providing targeted expertise in specific crime areas.

The overall objective of the Regulation is to strengthen cooperation between Member States' law enforcement authorities in preventing and combating serious cross-border crime and terrorism by improving information exchange, analytical capabilities and operational coordination at EU level.

In **2022**, Regulation (EU) 2022/991 introduced further amendments aimed at addressing emerging operational and technological challenges. These amendments strengthened cooperation between law enforcement authorities and private parties, enabled Europol to process large and complex datasets for criminal analysis, and enhanced the Agency's role in research and innovation related to security technologies. They also clarified Europol's ability to support investigations concerning crimes affecting a Union interest, even where a clear cross-border dimension is not initially established, and empowered Europol to propose the introduction of information alerts in the Schengen Information System (SIS) regarding third-country nationals involved in terrorism and serious crime.

The amended framework also strengthened cooperation between Europol and the European Public Prosecutor's Office (EPPO), operational since 2021. Europol's activities are organised around specialised centres focusing on specific crime areas, providing targeted operational and analytical support to Member States.

These developments progressively strengthened Europol's mandate and operational capabilities, positioning the Agency as the EU's central hub for criminal intelligence and operational coordination in the fight against serious cross-border crime and terrorism.

Figure 1: The evolution of Europol's mandate

Europol operates in a **rapidly evolving security environment**. Criminal networks increasingly operate across borders, exploiting differences between national legal frameworks, jurisdictional limits and gaps in information exchange between authorities. At the same time, they make extensive use of digital technologies, encrypted communications and global financial systems to facilitate and conceal their activities. These developments create significant challenges for national law enforcement authorities, which often face difficulties in obtaining timely cross-border information and coordinating investigations. In this context, Europol supports Member States in preventing and combating serious and organised crime, terrorism and other forms of cross-border criminal activity by providing analytical support, facilitating information exchange and supporting the coordination of cross-border investigations. Europol also contributes to the implementation of EU security priorities, as reflected in the ProtectEU Internal Security Strategy, including operational cooperation frameworks such as EMPACT.

The intervention logic underlying Regulation (EU) 2016/794 and its subsequent amendment by Regulation (EU) 2022/991 is based on the recognition that serious and organised crime and terrorism increasingly operate across national borders and require coordinated responses at EU level. By strengthening Europol's mandate, improving mechanisms for information exchange and criminal intelligence analysis, and enhancing operational coordination between national law enforcement authorities, the Regulation aims to increase the effectiveness of cross-border investigations and support Member States in addressing complex transnational crime threats. The intervention is

therefore expected to contribute to improved operational cooperation, more efficient use of law enforcement resources, and enhanced situational awareness at EU level, ultimately strengthening the Union's capacity to prevent and combat serious crime and terrorism while ensuring respect for fundamental rights.

This evaluation therefore examines the extent to which the existing legal framework has enabled Europol to fulfil these objectives, in particular by strengthening information exchange, analytical support and operational coordination between Member States in the fight against serious cross-border crime and terrorism.

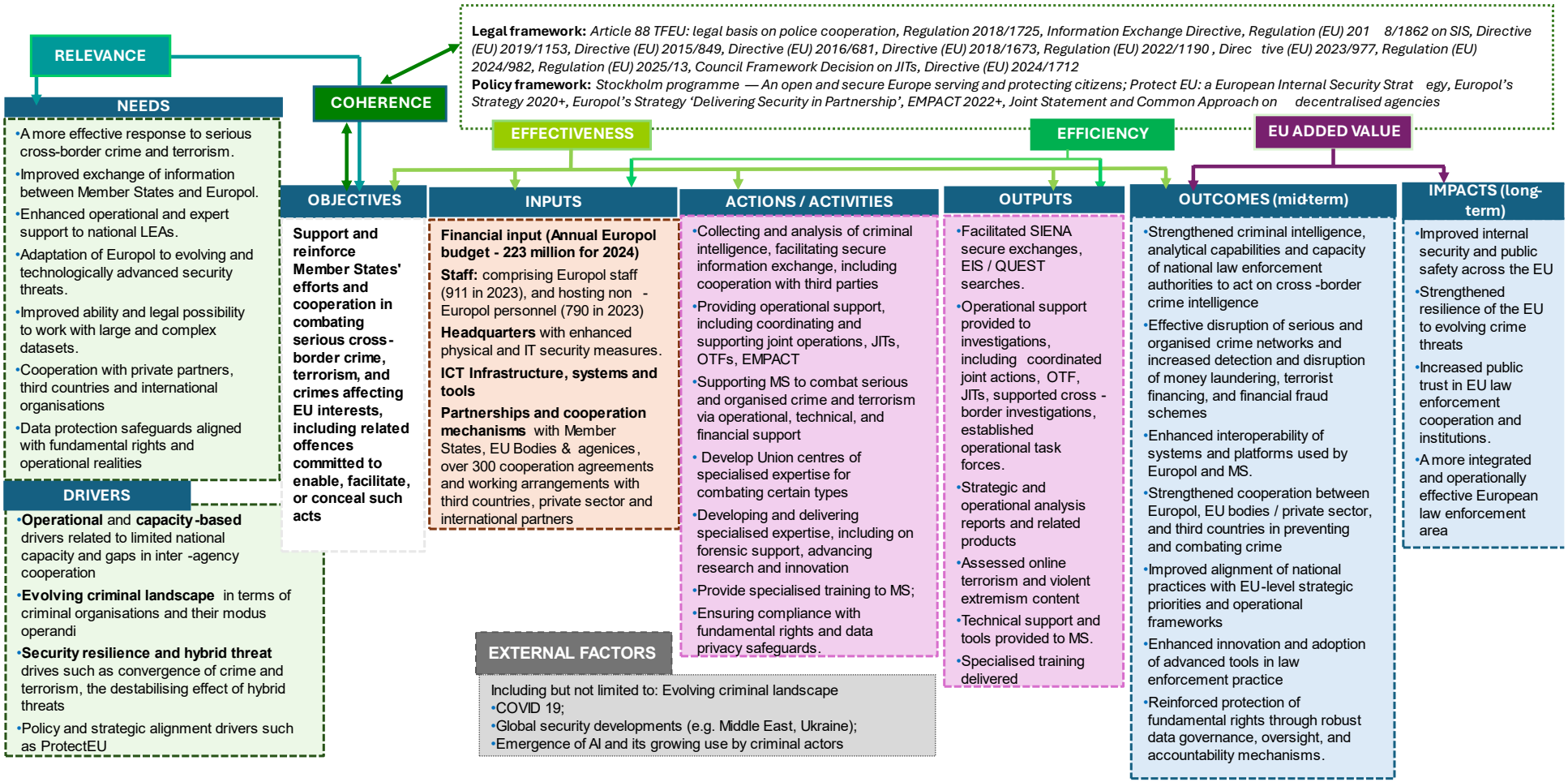


Figure 2: Intervention logic

2.2. Points of comparison

This section explains the points of comparison used to assess the impact of Regulation (EU) 2016/794 and its amendment by Regulation (EU) 2022/991 on Europol's functioning. The evaluation relies primarily on **temporal comparisons** between the situation prior to the adoption of the Regulation and developments observed during its implementation.

The main **baseline** for the evaluation is the situation before the entry into force of Regulation (EU) 2016/794, when Europol operated under the legal framework established by the 2009 Council Decision. This baseline provides a reference point for assessing how the 2016 Regulation strengthened Europol's governance framework, operational mandate and analytical capabilities.

The evaluation then examines developments during the implementation period of the Regulation, from its entry into force in 2017 to 2024. Within this period, particular attention is given to developments following the entry into force of Regulation (EU) 2022/991. This allows the evaluation to assess both the longer-term effects of the 2016 Regulation and the early impacts of the 2022 amendment.

To structure the analysis, the evaluation examines developments across **six core activity areas** reflecting Europol's main operational functions: information management, operational support, strategic analysis, specialised expertise through operational centres, cooperation with private sector entities and external cooperation with international partners. These activity areas serve as analytical benchmarks for assessing changes in Europol's operational output, use of information systems and support to Member States over the evaluation period.

In addition to temporal comparisons, the evaluation also considers **contextual benchmarks** in order to better understand Europol's role within the broader EU security architecture. This includes comparisons with other EU bodies involved in combatting cross-border crime, such as Frontex and the European Public Prosecutor's Office, as well as reference to international cooperation mechanisms, notably Interpol, in order to contextualise Europol's position as an EU-level criminal intelligence hub.

Finally, **thematic comparisons** are used to assess how Europol's activities have evolved in response to emerging crime threats. This includes examining developments in areas such as cybercrime, terrorism, human trafficking and financial crime, in order to determine whether the regulatory framework has enabled Europol to adapt its operational and analytical support to the evolving security environment.

Taken together, these points of comparison allow the evaluation to assess whether the current legal framework has strengthened Europol's operational effectiveness, improved information exchange and analytical support to Member States, and enhanced cooperation with relevant partners at EU and international level.

3. What was the expected outcome of the intervention?

The intervention evaluated in this report is **Regulation (EU) 2016/794**, which entered into force in May 2017 and established the current legal framework governing **Europol**. The Regulation replaced the framework established by **Council Decision 2009/371/JHA**, under which Europol had operated since 2010. The reform responded to the growing cross-border dimension of serious and organised crime and terrorism, which increasingly required more effective mechanisms for information exchange, criminal intelligence

analysis and operational coordination between Member States[166]. The need for the intervention was linked to limitations identified in the previous legal framework, including restrictions on Europol's ability to process operational data, support investigations and cooperate effectively with other EU bodies and external partners.

The general objective of the Regulation was to enhance cooperation between law-enforcement authorities in the Union and to strengthen support to Member States in preventing and combating serious and organised crime and terrorism affecting two or more Member States[167]. To achieve this objective, the Regulation clarified Europol's tasks and strengthened its mandate to provide criminal intelligence analysis, operational coordination and specialised support to investigations, as well as to manage EU-level information systems used for law-enforcement cooperation[168].

The intervention logic underlying the Regulation expected that strengthening Europol's mandate and analytical capabilities would lead to increased use of Europol's information systems, greater analytical and operational support provided to Member States' investigations and stronger coordination of cross-border law-enforcement actions. These outputs were expected to **improve the identification of links between criminal investigations conducted in different Member States** and facilitate coordinated investigations targeting organised criminal networks operating across jurisdictions[169]. Ultimately, the intervention was expected to contribute to strengthening the EU's capacity to combat serious and organised crime and terrorism with a cross-border dimension and to improve the effectiveness of law-enforcement cooperation across the Union. These objectives are also consistent with broader EU policy goals on internal security[170] and contribute indirectly to SDG 16 (peace, justice and strong institutions), particularly targets relating to combating organised crime and strengthening institutional capacity[171].

The evaluation therefore assesses whether these expected outputs, results and impacts materialised during the evaluation period 2017-2024 compared with the baseline situation under the previous legal framework between 2014 and 2016.

4. How has the situation evolved over the evaluation period?

4.1. Current state of play

This section describes how Europol's activities and operational capacity evolved during the evaluation period 2017-2024 following the entry into force of Regulation (EU) 2016/794. Developments are compared with the baseline period 2014-2016, when Europol operated under the legal framework established by the 2009 Council Decision.

---

[166] European Commission, *Proposal for a Regulation on the European Union Agency for Law Enforcement Cooperation (Europol)*, COM(2013) 173 final, 27.3.2013, explanatory memorandum; European Commission, *Impact Assessment accompanying the proposal for a Regulation on Europol*, SWD(2013) 98 final, 27.3.2013; Recitals 1-6 of Regulation (EU) 2016/794.
[167] Article 3 of Regulation (EU) 2016/794.
[168] Articles 4-7 and Articles 17-21 of Regulation (EU) 2016/794.
[169] SWD(2013) 98 final,
[170] European Commission, The EU Internal Security Strategy in Action, COM(2010) 673 final.
[171] A/RES/70/1, 2015.

During the evaluation period, Europol's activities developed across **three main areas**: information management, operational support and analytical capabilities, and cooperation with operational partners.

Information management

Europol acts as a **hub for criminal intelligence exchange** between EU law enforcement authorities. Secure operational communication is primarily conducted through the Secure Information Exchange Network Application (SIENA), supported by the Europol Information System (EIS) and the Querying Europol Systems (QUEST) interface. These systems enable national authorities to exchange operational messages, query data stored in Europol systems and identify links between investigations.

During the evaluation period, the volume of operational exchanges conducted through **SIENA increased steadily,** and its use also contributed to a rise in the number of operational cases. During the same period, the number of competent authorities connected to SIENA expanded to include national law enforcement authorities, customs administrations, and Police and Customs Cooperation Centres (PCCCs)[172].

SIENA			
Year	**Messages exchanged**	**Creation of operational cases**	**Connected authorities**
2016	869 858	46 437	757
2017	~1 million	66 113	1 100
2020	~1.3 million	88 748	2 239
2023	~1.8 million	151 318	2 950
2024	~2 million	169 500	**3 500**

Source: Europol operational statistics; Europol annual reports 2017-2024.

The expansion of SIENA connectivity took place in a **broader EU policy context** aimed at strengthening law enforcement information exchange[173]. During the evaluation period, the Union adopted new legislative measures in this area, including the Information

[172] The extent and timing of this integration varied across Member States. Member States with direct connections between national case-management systems and SIENA recorded higher volumes of automated exchanges, while others continued to rely primarily on manual message entry through central contact points or Europol National Units (External evaluation study, 2026).

[173] During the evaluation period, the Union adopted or developed several instruments relevant to police information exchange, including the Information Exchange Directive, Prüm II, the interoperability framework for EU information systems and the Digital Services Act, each of which created new interfaces or implementation tasks relevant to Europol's information-management and ICT environment. These developments affected the technical and organisational environment in which SIENA, EIS and related tools operated during the period under evaluation.

Exchange Directive[174], which provides for the mandatory use of SIENA by national Single Points of Contact and foresees the integration of SIENA into national police case-management systems. As the Directive was adopted towards the end of the evaluation period, its implementation had only started in several Member States by 2024 and the transitional arrangements for its application extend beyond the evaluation period. During the period covered by this evaluation, SIENA therefore remained one of several channels used by national authorities for cross-border law enforcement information exchange.

The operation of Europol's information-management environment during the evaluation period was also shaped by developments relating to data standardisation, large datasets and data protection. A large share of SIENA traffic continued to be transmitted in unstructured formats, including narrative text, PDFs, screenshots, scans and extracted device data, requiring manual handling before these data could be cross-checked or analysed[175]. The **UMF** initiative did not progress to full operational implementation during the evaluation period[176].

In addition to secure communication through SIENA, Europol maintains centralised criminal intelligence databases accessible to national authorities through the **Europol Information System (EIS)** and the **QUEST search interface**[177], which enables searches across multiple Europol datasets. This system allows national authorities to query operational data stored at Europol and identify potential links between criminal investigations conducted in different jurisdictions.

During the evaluation period, both the **volume of searches conducted in Europol systems** and the **number of data objects stored in the EIS** evolved as follows:

Year	EIS searches	EIS objects
2015	633 639	295 374
2016	1 436 838	395 357
2017	2 478 825	1 062 236
2020	10 231 771	1 337 089
2023	14 238 667	1 572 837

[174] Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA.
[175] External evaluation study supporting the evaluation and impact assessment of Regulation (EU) 2016/794, 2026.
[176] External evaluation study supporting the evaluation and impact assessment of Regulation (EU) 2016/794, 2026.
[177] The development and use of EIS and QUEST during the evaluation period depended on how national authorities connected their domestic systems to Europol's tools. Many Member States continued to use SIENA to request EIS cross-checks, as QUEST or other automated loaders had not yet been implemented. Data provision to EIS also remained uneven, with structured uploads, automated ingestion, and common formats not uniformly implemented across the Union. (External evaluation study, 2026).

2024	12 795 330	1 693 143

Source: Europol

Europol also performs automated **cross-matching of operational data** received from Member States in order to identify potential links between criminal investigations conducted in different jurisdictions. This process generates crossmatch reports and SIENA hit notifications that are transmitted to the relevant national authorities when matches are detected between datasets stored in Europol systems.

During the evaluation period, the number of crossmatch reports and hit notifications generated by Europol evolved as follows: 7 372 in 2017, 6 824 in 2018, 7 806 in 2019, 9 559 in 2020, 14 413 in 2021, 14 737 in 2022, and 14 407 crossmatch reports in 2023, followed by 13 409 reports in 2024[178].

A key development affecting information management during the evaluation period concerned the handling of large and complex datasets. Regulation (EU) **2022/991** clarified Europol's legal framework for processing personal data received without data-subject categorisation for the purpose of completing categorisation and supporting ongoing investigations. Under Article 18(6a), such data may be processed for up to **18 months**, extendable to **36 months in justified cases**, solely for completing data-subject categorisation. Article 18a introduced a derogation allowing Europol to process personal data from competent authorities, the EPPO or Eurojust, where necessary to support ongoing criminal investigations, including through operational analysis and, in exceptional and duly justified cases, cross-checking. These amendments required the development of internal procedures and data-governance arrangements for the management of large and complex datasets.

Operational support and analytical capabilities

Europol provides operational support to Member States in cross-border investigations and operational actions through analytical support, operational coordination and specialised technical expertise. Under Regulation (EU) 2016/794, Europol supports national authorities by providing criminal intelligence analysis, coordinating operational activities and deploying specialised capabilities during investigations. These activities include support to operational investigations, participation in Joint Investigation Teams (JITs), organisation of operational meetings, support to Operational Task Forces (OTFs), coordination of Joint Action Days (JADs) and the deployment of mobile offices and specialised staff during operational actions.

During the baseline period (2014-2016), Europol already provided operational analytical support to Member States primarily through **Analytical Work Files (AWFs)**, operational meetings and participation in Joint Investigation Teams (JITs). AWFs were the main analytical structures used by Europol to analyse operational data and support cross-border investigations[179]. Europol also facilitated coordination between national authorities

[178] Europol Consolidated annual activity reports.
[179] Council Decision 2009/371/JHA establishing the European Police Office (Europol), OJ L 121, 15.5.2009, Articles 10-14.

through operational meetings and analytical support to investigations[180]. According to Europol operational statistics, the Agency produced around **5 300 operational reports in 2016**, reflecting the analytical support provided to national investigations during this period[181]. Operational support during the baseline period was therefore primarily focused on providing criminal intelligence analysis and facilitating coordination between national authorities involved in cross-border investigations.[182]

Following the entry into force of **Regulation (EU) 2016/794** in 2017, Europol's operational support was progressively expanded and became increasingly structured around intelligence-led investigations targeting organised criminal networks operating across several Member States. This reflected the strengthened mandate of Europol to provide analytical support, operational coordination and specialised expertise to national authorities in cross-border investigation. During the evaluation period, operational coordination increasingly relied on structures such as Operational Task Forces (OTFs)[183] and Europol's participation in Joint Investigation Teams (JITs)[184], which bring together investigators and analysts from several Member States to support intelligence-led investigations targeting priority criminal networks. Europol also supports coordinated operational actions between Member States through the organisation of **Joint Action Days**[185]. The number of JADs has increased throughout the evaluation period, with a total of 7 taking place in 2017, 10 in 2023 and 11 in 2024.[186]

Year	Cross-border investigations supported by Europol	Joint Investigation Teams	Operational Task Forces
2014-2016 (baseline annual average)	~1 000	38 JITs	-
2017	1496	61 JITs	-
2020	837	57 JITs (including 15 newly signed)	11

[180] Europol, Annual General Report 2015, The Hague, 2016.
[181] Europol, Consolidated Annual Activity Report 2016, The Hague, 2017, p. 12.
[182] Europol, Consolidated Annual Activity Report 2016, pp. 11–14.
[183] Operational Task Forces are operational coordination structures supported by Europol that bring together investigators and analysts from several Member States to target priority criminal networks and conduct intelligence-led investigations.
[184] Joint Investigation Teams are cooperation mechanisms enabling competent authorities from two or more countries to conduct joint criminal investigations for a specific purpose and limited period. Europol supports JITs by providing analytical, operational and coordination assistance.
[185] These operations involve coordinated law enforcement activities carried out simultaneously in several Member States and supported by Europol through operational coordination, criminal intelligence analysis and mobile office deployment. They take place in the framework of EMPACT.
[186] Europol, Consolidated Annual Activity Reports 2017, 2023, 2024.

2023	3155	33 JITs (including 21 newly initiated teams)	27
2024	3 324	49 JITs (including 36 newly established).	65[187]

Source: Europol operational statistics

In parallel with the increase in investigations supported, Europol's analytical output expanded considerably during the evaluation period**. Operational reports** produced in direct support of investigations increased from 5 330 in 2016 to 23 012 in 2023 and 21 281 in 2024. Europol also continued to produce **strategic analysis**[188] on emerging crime threats and supporting EU operational frameworks such as EMPACT. In 2024, Europol produced 29 strategic analysis reports and 366 operational analysis reports, compared with 44 strategic reports and 332 operational reports in 2017.

At the same time, the **speed of operational analytical responses improved substantially** over the evaluation period. Europol operational data indicate that the average response time to analytical requests from Member States decreased from 27.5 days in 2016 to a range of 3-4 days between 2021 and 2024. In 2024, the average turnaround time for 80% of first-line analysis requests was 3.2 days, compared with 4.2 days in 2023.

A further component of Europol's operational support consists of **on-the-spot operational deployments**, primarily through the use of mobile offices[189] and the deployment of specialised operational staff. During the baseline period (2014-2016), Europol already provided such support during investigations and operational actions. In 2016, Europol recorded **159 short-term mobile office deployments, 56 long-term deployments and 6 permanent deployments** supporting operational activities[190]. Mobile offices were also deployed during major investigations, for example to support operations in Belgium and France following the 2015-2016 terrorist attacks[191].

During the evaluation period, the number of deployments increased significantly, reaching 339 in 2017, 370 in 2018 and 353 in 2019[192]. While reporting categories changed slightly over time, the figures indicate a substantial increase in the use of mobile offices to provide on-the-spot analytical support during operational actions.

---

[187] In 2024, Europol also introduced a new internal management and monitoring framework for OTFs (OTF.360), although the operational impact of this new framework falls largely beyond the evaluation period.
[188] Europol's analytical products include the Serious and Organised Crime Threat Assessment (SOCTA), the Internet Organised Crime Threat Assessment (IOCTA), the EU Terrorism Situation and Trend Report (TE-SAT) and the European Financial and Economic Crime Threat Assessment (EFECTA).
[189] Mobile offices allow investigators to access Europol databases and analytical tools in real time during operational actions and enable the immediate cross-checking of operational data against information stored in Europol systems.
[190] Europol Consolidated Annual Activity Report 2016.
[191] Europol Review 2016-2017.
[192] Europol, Consolidated Annual Activity Reports 2017–2019. Mobile offices were also used to support major international security events requiring enhanced operational coordination. In 2024, for example, Europol provided operational support during UEFA EURO 2024 and the Paris 2024 Olympic and Paralympic Games, including the deployment of staff and coordination support.

During the **evaluation period (2017-2024)**, Europol further expanded its specialised operational structures to address evolving crime threats[193]. The **European Counter Terrorism Centre (ECTC)**, launched in **2016**, strengthened operational coordination and information exchange between Member States in terrorism investigations. In **2020**, Europol established the **European Financial and Economic Crime Centre (EFECC)** to enhance support for investigations related to financial and economic crime, including fraud, corruption, money laundering and asset recovery.

Technological developments increasingly shaped Europol's operational capabilities during the evaluation period, reflecting the growing importance of digital evidence and large datasets in criminal investigations. While Europol already used analytical tools to support investigations during the **baseline period**, it did not yet have dedicated innovation structures or programmes to develop new technological capabilities. The expansion of cybercrime, online fraud, encrypted communications and cryptocurrency-related crime therefore led to growing demand from Member States for advanced data-analysis tools, prompting Europol to progressively strengthen its technological capacities and establish dedicated innovation structures.

In this context, Europol created the **Europol Innovation Lab** in 2020 to develop and test new technologies relevant for law enforcement, including artificial intelligence, data mining and advanced analytics applied to large operational datasets[194]. In 2024, Europol further strengthened these capabilities with the launch of the **Research and Innovation Sandbox**, which allows the development and testing of AI models using operational datasets under controlled conditions. These developments illustrate a broader shift during the evaluation period towards **data-driven investigations**, in which large volumes of digital evidence and financial data increasingly require specialised analytical tools and technological expertise to support cross-border investigations.

In addition to supporting Member States directly, Europol provides **operational and analytical support within the broader EU internal security architecture** through cooperation with EU agencies and bodies involved in law-enforcement, border management and judicial cooperation.

During the **baseline period (2014-2016)**, operational cooperation between Europol and other EU actors already existed[195], particularly with **Eurojust** in the context of Joint Investigation Teams (JITs). In 2016, 50 operational cases supported by Europol involved Eurojust, reflecting the complementary analytical and judicial support provided by the two agencies in cross-border criminal investigations[196]. Cooperation also took place with **Frontex**, particularly in investigations related to migrant smuggling and cross-border

[193] Some of these structures were already operational during the baseline period (2014-2016). The European Cybercrime Centre (EC3), established in 2013, supports investigations related to cybercrime, online fraud and child sexual exploitation and provides specialised capabilities such as digital forensics, malware analysis and cryptocurrency tracing. In 2016, Europol created the European Migrant Smuggling Centre (EMSC) to strengthen support to Member States in investigations targeting migrant smuggling networks.

[194] By 2023, the Innovation Lab had supported dozens of innovation projects and research initiatives involving law enforcement authorities, EU agencies, research institutions and private-sector partners, and contributed to the development and testing of analytical tools made available to the European policing community through Europol's tool repository, which hosts more than 30 investigative tools.

[195] Cooperation was primarily based on operational coordination, participation in joint meetings and information exchange through Europol systems.

[196] Europol, Consolidated Annual Activity Report 2016.

organised crime. In 2016, Europol deployed officers to migration hotspot locations in Greece and Italy to support operations coordinated by Frontex and assist Member States in identifying criminal networks involved in migrant smuggling[197].

During the **evaluation period (2017-2024)**, this cooperation expanded as the EU internal security architecture evolved and new actors were created. Europol increasingly contributed analytical support, operational coordination and information exchange to **multi-agency investigations and EU-level operational frameworks**.

One important development was the establishment of the **European Public Prosecutor's Office (EPPO)[198],** operational since **2021**, which investigates crimes affecting the EU's financial interests. Europol provides analytical support and intelligence cross-checks in investigations related to fraud, corruption and other financial crimes affecting the EU budget. Europol contributes to a subset of these investigations by providing **analytical support, cross-matching of operational data and intelligence analysis**, particularly in complex cases involving organised fraud schemes, corruption and cross-border VAT fraud affecting the EU budget. Europol supported six EPPO cases in 2021, 28 cases in 2022, 47 cases in 2023 and 83 cases in 2024. Cooperation with EPPO increased gradually during the latter part of the evaluation period as operational arrangements between the two organisations were implemented.

Europol also contributed to training and knowledge-sharing activities for law enforcement authorities. During the evaluation period, Europol cooperated with the **European Union Agency for Law Enforcement Training (CEPOL)** to deliver training programmes addressing priority crime areas such as cybercrime, financial crime and counterterrorism. In **2024**, more than **800 law enforcement officers** participated in Europol-supported training activities.

The implementation of this support to EU agencies and EU-level frameworks developed progressively during the evaluation period and was influenced by differences in institutional mandates, data access conditions and the maturity of inter-agency working arrangements. The focus group with EU agencies and bodies noted that cooperation is often operationally close, but that data protection arrangements, mandate boundaries and data ownership principles continue to shape how information can be exchanged and used across institutional actors. These factors formed part of the operational context in which Europol's support functions evolved over the period.

External cooperation

Cooperation with external partners strengthened over the evaluation period, reflecting the **increasing international dimension of serious and organised crime** and the operational needs of Member States to cooperate with partners outside the EU.

During the baseline period (2014-2016), Europol already maintained **cooperation agreements** with around 25 third countries and international organisations and hosted around 200 liaison officers at it headquarter.

During the evaluation period, Europol further expanded its external cooperation network. The Agency concluded additional working arrangements with third countries and partners,

[197] Europol, Consolidated Annual Activity Report 2016.
[198] Regulation (EU) 2017/1939.

including **Singapore in 2020** and **India in 2023**, and strengthened operational cooperation with international organisations such as **INTERPOL** and **International Criminal Court**. In parallel, Europol increasingly cooperated with private-sector partners, particularly in cybercrime and online fraud investigations. By the early 2020s, Europol was working with **a large number of private-sector partners**, including technology companies and financial institutions, in public-private partnerships supporting investigations related to cybercrime and illicit financial flows.

The pace of developments in external cooperation during the evaluation period was influenced by several factors. The growing transnational nature of criminal networks created increased demand from Member States for cooperation with third countries and international partners. At the same time, the development of formal cooperation frameworks depends on the existence of an appropriate legal basis under the Europol Regulation, including international agreements between the EU and partner countries where the exchange of personal data is envisaged. The negotiation and adoption of such agreements require compliance with EU data protection standards and fundamental rights safeguards and may therefore take time. In addition, broader EU external security priorities and the strategic importance of certain partner countries also shaped the development of Europol's external cooperation network.

5. Evaluation findings

5.1. To what extent was the intervention successful and why?

The success of the intervention is assessed in terms of the extent to which the Regulation strengthened cooperation between Member States' law enforcement authorities in preventing and combating serious cross-border crime and terrorism, and whether this was achieved effectively, efficiently and in a coherent manner within the EU internal security framework.

Effectiveness

Effectiveness concerns the extent to which the objectives of the Regulation have been achieved.

The expected outcome of the intervention was to strengthen operational cooperation between Member States through improved information exchange, enhanced analytical capabilities and stronger operational coordination at EU level. Evidence presented in Section 2 indicates that **these objectives have been largely achieved** during the evaluation period.

Operational data[199] show a substantial increase in the use of Europol's information exchange infrastructure. The volume of operational exchanges through the Secure Information Exchange Network Application (SIENA) increased significantly during the evaluation period, reaching approximately **two million messages in 2024**. Similarly, the number of searches conducted in Europol's information systems increased substantially over the same period. These developments suggest that national law enforcement authorities **increasingly rely on Europol's systems** to support cross-border investigations.

[199] Europol Annual Reports 2017-2024.

Evidence from stakeholder consultations supports this finding. Respondents to the Commission's public consultation[200] consistently identified Europol's role in facilitating cross-border information exchange and operational coordination as one of the Agency's **most important contributions to EU law enforcement cooperation**. Focus group discussions with Member State authorities[201] similarly emphasised the **operational importance of Europol's** information exchange systems and analytical support. Participants indicated that Europol's analytical capabilities frequently enable investigators to identify links between criminal cases conducted in different jurisdictions and facilitate coordinated operational actions across Member States.

Operational support provided by Europol has also expanded significantly during the evaluation period. The number of cross-border investigations supported by Europol increased substantially, reaching approximately 3 324 investigations supported in 2024[202]. Case studies analysed during the external evaluation[203] study demonstrate that Europol's **analytical capabilities frequently enable investigators to identify links** between criminal cases in different Member States and facilitate coordinated operational action against transnational criminal networks.

The development of **specialised operational centres** within Europol also contributed to strengthening operational effectiveness. Centres such as the European Cybercrime Centre (EC3), the European Counter Terrorism Centre (ECTC) and the European Financial and Economic Crime Centre (EFECC) provide specialised expertise in areas such as digital forensics, financial investigations and counter-terrorism intelligence analysis[204]. Stakeholder consultations[205] indicate that these specialised capabilities are particularly valuable for Member States with more limited technical resources.

Despite these positive developments, the evaluation identified several factors that may affect the full effectiveness of the intervention.

First, evidence collected through focus group discussions[206] indicates that **information sharing practices remain uneven** across Member States. Some Member States contribute significantly larger volumes of operational data than others, which may affect the completeness of operational datasets available to Europol for analytical purposes.

Second, stakeholders[207] highlighted **operational challenges related to the processing of large and complex datasets**, particularly in cases involving digital evidence and encrypted communications.

Third, consultations identified procedural constraints related to data protection requirements and data ownership principles that may affect Europol's ability to process certain datasets or share information across institutional boundaries (EU agencies focus group, January 2026).

---

[200] Public consultation summary report, 2026.
[201] Member States focus group, January 2026.
[202] Europol Annual Reports 2017-2024.
[203] External evaluation study, 2026.
[204] Europol Annual Reports 2017-2024.
[205] Public consultation summary report, 2026.
[206] Member States focus group, January 2026.
[207] EU agencies focus group, January 2026.

Overall, the available evidence indicates that the Regulation has significantly strengthened operational cooperation between Member States and enhanced Europol's role as the EU's central criminal intelligence hub.

Efficiency

Efficiency assesses whether the objectives of the intervention were achieved at reasonable cost and whether the available resources were used proportionately to the results obtained.

Europol provides several centralised services at EU level, including secure communication systems, analytical platforms and specialised forensic capabilities. These services allow Member States to pool resources and **avoid duplicating** similar infrastructure at national level.

The expansion of Europol's operational activities during the evaluation period occurred alongside increases in the Agency's financial and human resources. Overall, the available evidence indicates that Europol's operational outputs have increased broadly in line with the growth in available resources[208].

Year	Budget	Staff
2016	€104.9 million	655
2017	€129.9 million	684
2018	€136.1 million	859
2019	€138.3 million	893
2020	€143.6 million	871
2021	€168.8 million	960
2022	€192.4 million	992
2023	€200 million	911
2024	€217 million	941

Evidence from stakeholder consultations[209] suggests that Europol's centralised services generate **economies of scale** by providing specialised analytical and technical capabilities that would be costly for individual Member States to develop independently.

Focus group discussions with Member States[210] indicate that measures aimed at strengthening automated data exchange and systematic use of Europol systems could generate significant operational benefits while involving moderate implementation costs.

At the same time, consultations indicate that increasing demand for Europol's services may place pressure on the Agency's analytical capacity and operational resources[211].

[208] Europol Annual Reports 2017-2024.
[209] Public consultation summary report, 2026.
[210] Member States focus group, January 2026.
[211] External evaluation study, 2026.

Stakeholders[212] also identified opportunities to improve efficiency by simplifying certain operational procedures, strengthening interoperability between information systems and improving digital tools supporting operational cooperation.

Overall, the evaluation indicates that Europol's services contribute to more efficient use of law enforcement resources across the Union, although growing operational demand may require additional resources to maintain this level of efficiency.

Coherence

Coherence assesses whether the intervention is consistent with other EU policies and instruments and whether it interacts effectively with the broader EU internal security framework.

Europol operates within a broader EU security architecture that includes several actors involved in law enforcement cooperation and judicial coordination, including Eurojust, the European Public Prosecutor's Office (EPPO), Frontex and CEPOL.

Evidence collected during the evaluation[213] indicates that Europol's activities **generally complement those of these actors**, particularly through its role in providing criminal intelligence analysis and facilitating information exchange between national authorities and other EU Agencies, bodies and offices. In particular, Europol plays an important role in supporting the European Multidisciplinary Platform Against Criminal Threats (EMPACT), which coordinates operational actions against priority crime threats at EU level.

At the same time, consultations with EU agencies[214] highlighted certain operational challenges related to the interaction between different institutional mandates and legal frameworks. In particular, stakeholders noted that differences in data protection frameworks and institutional mandates may affect the efficiency of information exchange between EU bodies.

Nevertheless, the evaluation did not identify major inconsistencies between the Europol Regulation and other EU legal instruments.

5.2. How did the EU intervention make a difference?

This section assesses the **EU added value** of the intervention. EU added value refers to the benefits generated by EU-level intervention that would not have been achieved, or would have been achieved less effectively, by Member States acting individually.

The evaluation finds that Europol **generates substantial EU added value** by enabling the integration of criminal intelligence and operational coordination across multiple Member States.

Europol's centralised information exchange infrastructure enables national authorities to share operational information simultaneously with multiple partners, facilitating the identification of links between criminal investigations conducted in different Member

[212] EU agencies focus group, January 2026.
[213] External evaluation study, 2026.
[214] EU agencies focus group, January 2026.

States [215]. Without EU-level coordination mechanisms such as those provided by Europol, cooperation between national authorities would rely primarily on bilateral exchanges, which may be slower and less effective in addressing complex transnational criminal networks. Stakeholder consultations[216] indicate that Europol's analytical and coordination capabilities significantly **enhance the effectiveness of cross-border investigations compared with bilateral cooperation mechanisms**.

Europol also centralises specialised analytical and technical capabilities at EU level, including advanced digital forensic tools, financial intelligence analysis and cybercrime investigation support. By pooling these capabilities, Europol allows Member States to benefit from economies of scale and reduces the need for duplicative investment in specialised infrastructure[217].

These capabilities are particularly valuable for smaller or resource-constrained Member States[218].

Operational case studies analysed during the evaluation[219] show that Europol's analytical and coordination capabilities can play a decisive role in complex investigations targeting criminal networks operating across several jurisdictions.

Europol also facilitates cooperation between EU law enforcement authorities and international partners. Consultations with external stakeholders indicate that Europol serves as an important gateway for cooperation with the European Union, reducing the need for multiple bilateral contacts with individual Member States[220].

High-level stakeholders[221] also emphasised Europol's central role in facilitating information exchange and analytical cooperation across the Union.

Overall, the evaluation concludes that the intervention provides clear EU added value by enabling coordinated operational responses to cross-border criminal threats that would be significantly more difficult to achieve through national or bilateral cooperation mechanisms alone.

5.3. Is the intervention still relevant?

The relevance criterion assesses whether the objectives of the intervention remain appropriate in the context of evolving crime threats and operational needs.

Evidence from Europol threat assessments[222] indicates that organised crime groups increasingly operate across national borders and rely heavily on digital technologies, encrypted communication services and global financial systems to conduct illicit activities.

---

[215] Europol Annual Reports 2017-2024.
[216] Public consultation summary report, 2026.
[217] External evaluation study, 2026.
[218] Public consultation summary report, 2026.
[219] External evaluation study, 2026.
[220] External evaluation study, 2026.
[221] Joint Statement by the European Police Chiefs on the Future Development of Europol.
[222] SOCTA, 2025.

Stakeholder consultations conducted during the evaluation[223] indicate strong support for Europol's role in facilitating cross-border operational cooperation and providing analytical support to Member States. In particular, respondents to the public consultation and call for evidence emphasised the growing importance of EU-level coordination mechanisms in addressing technologically sophisticated forms of criminal activity, including cybercrime and online financial fraud[224].

Focus group discussions with Member States and EU agencies[225] highlighted the **increasing importance of EU-level coordination mechanisms** in addressing technologically sophisticated forms of criminal activity, including cybercrime and online financial fraud. Focus group discussions[226] similarly highlighted the increasing complexity of criminal investigations involving digital evidence, large datasets and cross-border financial flows.

At the same time, stakeholders identified areas where evolving operational needs may require further adaptation of the legal framework. These include:

- the increasing volume of digital evidence in criminal investigations
- the need to process large and complex datasets
- the growing importance of cooperation with private sector actors
- the rapid technological evolution of criminal methods.

Overall, the evaluation finds that **the objectives of Regulation (EU) 2016/794 remain highly relevant**, as the increasingly transnational and digital nature of serious crime continues to require strong EU-level mechanisms supporting operational cooperation between Member States.

6. What are the conclusions and lessons learned

6.1. Conclusions

The evaluation concludes that Regulation (EU) 2016/794 has **substantially strengthened** the European Union's capacity to prevent and combat serious and organised crime and terrorism with a cross-border dimension. Europol has consolidated its role as a central operational and analytical hub within the EU's internal security architecture, providing clear added value to Member States' law enforcement cooperation.

The evidence presented in Sections 3 and 4 indicates that the intervention has **largely achieved its objectives**. Europol has enhanced the quality, scale and intensity of cross-border information exchange and operational coordination among Member States. The growing use of Europol's information systems, notably SIENA and the Europol Information System, illustrates the increasing reliance of national authorities on Europol as a platform for secure information exchange and analytical support. Europol's strategic threat assessments, including SOCTA, IOCTA and TE-SAT, have become key tools for identifying EU crime priorities and informing operational planning at EU level.

[223] Public consultation summary report, 2026.
[224] Public Consultation Factual Summary Report, 2026; Call for Evidence Factual Summary Report, 2026.
[225] Member States focus group, January 2026; EU agencies focus group, January 2026.
[226] EU Agencies Focus Group Summary, February 2026.

Europol's specialised centres, such as the European Cybercrime Centre (EC3) and the European Counter Terrorism Centre (ECTC), have strengthened the Union's capacity to address emerging and technically complex threats by providing specialised expertise and analytical capabilities that many Member States could not sustain independently. In addition, Europol's operational support to mechanisms such as Joint Investigation Teams (JITs), Joint Action Days (JADs) and Operational Task Forces (OTFs) has facilitated coordinated enforcement actions, accelerated evidence collection and reduced duplication of investigative efforts across jurisdictions.

The evaluation also finds that Europol operates efficiently by centralising specialised ICT systems, analytical capabilities and operational coordination at EU level, generating economies of scale that individual Member States would struggle to achieve alone. Increased resources have enabled Europol to expand its outputs, particularly in information exchange and operational support. However, the continued growth in operational demand and the increasing complexity of transnational crime create pressures on Europol's resources and risk shifting the balance towards reactive operational support at the expense of strategic foresight.

The evaluation also finds that the intervention contributed to strengthening Europol's role within the EU internal security architecture. Cooperation between Europol and other EU actors, including **Eurojust**, **Frontex**, **European Public Prosecutor's Office** and **CEPOL**, expanded during the evaluation period. Europol also increased its engagement with international partners and private-sector actors in areas such as cybercrime and online fraud.

The Regulation remains **highly relevant to the evolving security landscape**. Serious and organised crime and terrorism continue to operate increasingly across borders, with digitalisation further expanding the scale and reach of criminal activities. Europol's mandate remains broadly aligned with these challenges, although emerging threats such as large-scale cyber-enabled fraud and the use of artificial intelligence in criminal activities may require further adaptation of the legal framework.

The evaluation finds that the Regulation is coherent both internally and with the broader EU legal framework governing police cooperation. Europol's mandate complements other EU instruments and agencies, contributing to a more integrated European security architecture while maintaining safeguards for fundamental rights.

Finally, the evaluation confirms that Europol generates **clear EU added value**. By providing EU-wide criminal intelligence, facilitating operational coordination and enabling cooperation with private sector partners and third countries, Europol supports a more coherent and effective European response to transnational crime. These benefits are particularly significant for smaller Member States that may lack the capacity to develop comparable capabilities at national level. At the same time, Europol's effectiveness continues to depend on the timely and comprehensive sharing of information by Member States, highlighting the importance of sustained engagement across the EU law enforcement community.

6.2. Lessons learned

Several lessons emerge from the evaluation.

First, the evaluation confirms the **continued importance of EU-level mechanisms for criminal intelligence exchange and operational coordination**. The transnational nature of serious and organised crime means that effective investigations increasingly require structured cooperation between multiple jurisdictions. Europol's systems and analytical capabilities play a central role in enabling such cooperation.

Second, the evaluation highlights the **growing importance of advanced analytical capabilities and technological tools** in criminal investigations. The increasing volume of digital evidence and the use of encrypted communications by criminal networks require specialised expertise and technological capabilities. The development of innovation-related initiatives within Europol during the evaluation period reflects the need to adapt operational support to these technological developments.

Third, the evaluation underlines the importance of **consistent and systematic information sharing** between Member States. Differences in data-sharing practices may reduce the completeness of operational datasets and limit the effectiveness of analytical support. Stakeholders emphasised that more systematic use of Europol systems and automated data exchange could further improve operational cooperation.

Fourth, the evaluation highlights the importance of **coherence across the EU internal security framework**. Effective cooperation between Europol and other EU actors depends on clear mandates, compatible data-protection frameworks and efficient mechanisms for information exchange. While cooperation between agencies is generally effective, stakeholders noted that differences in legal frameworks may sometimes affect operational coordination.

Finally, from a REFIT perspective, the evaluation suggests that **simplifying operational procedures and improving interoperability between information systems** could reduce administrative burden and increase efficiency. Stakeholders identified opportunities to streamline certain operational processes and strengthen digital tools supporting information exchange and analytical cooperation.

Overall, the evaluation indicates that the legal framework established by the Europol Regulation continues to provide a relevant basis for supporting Member States in addressing serious and organised crime and terrorism with a cross-border dimension. The lessons identified in this evaluation may inform future reflections on how EU-level mechanisms for law-enforcement cooperation can continue to adapt to evolving security threats and operational needs.

Table 1: Evaluation Matrix

Evaluation questions				
A	**Effectiveness: To what extent has Europol progressed positively towards achieving the objectives under its mandate?**			
	Sub-questions	**Judgment criteria**	**Indicators**	**Data collection tools and methods**
		Based on data and in the views of 'stakeholders'[227]		
1	To what extent have Europol's activities contributed to achieving the objectives under its regulatory framework to **support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime** affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a	Europol's contribution to ending ongoing or preventing cross-border serious and organised crime and terrorism is significant in terms of successful police interventions and operational results. Europol and Member States Law Enforcement Authorities (LEAs) cooperation is effective	**Qualitative:** Alignment of Europol's operations and activities with its policy objectives and priorities. **Opinion based:** Stakeholders' satisfaction level with Europol's activities and objectives.	**Desk research:** Data on evolution of serious and organised crime and terrorism and successful operations with the support of Europol, place into context crime areas in focus (Annex 1 Europol Reg). **Interviews:** Europol MB, Member States Ministry of Interior (political level); network of national parliament representatives reviewing report

[227] Unless otherwise specified, the term stakeholders indicate all categories consulted as indicated in the last column.

	Union policy and ensure security in the Area of Freedom, Security and Justice?	Resources allocated to Europol and their employment by the Agency meets the needs of MS and allows to swiftly address all requests for support by Member States law enforcement authorities. There is satisfaction with Europol's support	Stakeholders' perception of the pertinence of the EU policy objectives and related priorities. Member States law enforcement authorities' satisfaction with responsiveness of Europol. **Quantitative:** Overview of statistics on criminality in focus (Eurostat, UN survey of crime threads, JRC counter-terrorism knowledge hub, EU database of terrorist offenders etc) where available (limited information of cross-border crime), data from SIENA reports.	from Europol (Joint Parliamentary Scrutiny Group (JPSG)). **Survey:** Member States law enforcement authorities, General public, COM and EU agencies and bodies
2	To what extent have **Europol's activities** supported relevant **EU policy objectives and priorities related to the Area of Freedom, Security and Justice (specifically TFEU Art 67 (3); Art 87, 88)? (ER Art. 4.1 (j), (l); (u); (z); 4.2; 4.3; 4.4)**	Evolution of Europol's strategic contributions to cross-border police cooperation, support for judicial collaboration, and combatting serious crime and terrorism.	**Qualitative:** Alignment of EU operations with policy objectives and priorities. **Opinion based:**	**Desk research:** Europol strategic reports on evolution of crime, input to policy development. **Interviews:** Commission representatives of Europol Management Board, Member

		Measurement of improvements in the speed, efficiency, and success rates of joint operations, intelligence sharing, and coordination among Member States (Article. 4.2). Cooperation between Europol and Member State law enforcement authorities is considered effective Evidence of concrete outcomes, such as dismantling criminal networks, successful counterterrorism initiatives, and enhanced security measures. Europol successfully facilitated cooperation between law enforcement and judicial authorities across Member States	Stakeholders' satisfaction levels with Europol's activities and objectives. Stakeholders' perception of EU policy objectives and related priorities. **Quantitative:** Statistical data to measure operational success against crime and in supporting security – using EU-SOCTA, iOCTA, TE-SAT data, EMPACT reporting and specific early warning notifications, SIENA data	States, Ministries of Interior (political level), JSPG, Commission services, including SG, DG HOME, DG JUST coordination unit, Police Chiefs, HENU. **Survey:** Member State law enforcement authorities, EU agencies and bodies; General public (public consultation). **Comparative analysis:** with the operational records of other EU agencies, Member State law enforcement authorities and INTERPOL.

		Europol's input into EU policy development through strategic analysis a, recommendation, and dissemination of good practices to Member States and EU agencies. There is satisfaction with Europol's role in the EU architecture.		
3	To what extent did Europol's **priorities** and objectives set respectively by the **multi-annual programming** and the **annual work programmes** adopted by Europol Management Board (MB) between 2017-2024 reflect over time the overall priorities and **objectives of the Agency under its legal mandate**? (Article. 3)	Consistency between the priorities and objectives across the multi-annual programming, annual work programmes, and Europol's legal mandate and obligations resulting from other legal acts. Alignment of the programmes' goals with the overarching strategic goals of the Agency and the evolving political and legislative landscape.	**Qualitative:** Evidence of main initiatives or projects within the multi-annual and annual programmes adopted by the MB to illustrate how they contribute to the Agency's objectives under its legal mandate. Identified consistencies or discrepancies in the stated priorities and objectives. **Opinion based:**	**Desk research:** Review of grey literature (notably, Europol's operational documents such as SPDs and CAARs); mapping priorities against Annex 1 listed crimes **Interviews:** Member States Ministries of Interior/political level, JSPG, COM strategic staff JHA policy, Europol MB **Survey:** Member State law enforcement authorities, EU agencies and bodies; General public (public consultation)

			Effectiveness of the multi-annual programming and the annual work programmes adopted by Europol MB in meeting the Agency's objectives under its legal mandate. **Quantitative:** Review of performance indicators and data and progress reports to measure the progress and achievements over the evaluation period (2017-2024).	
4	To what extent and how have **external factors** (COVID, development of AI and other technology; global security developments) influenced the effectiveness of Europol?	External factors had limited impact on Europol's objectives and tasks. External factors had limited impact on the effectiveness of Europol's working methods.	**Qualitative:** Identification and assessment of external factors impacting Europol's operational effectiveness. **Opinion-based:** Perceptions of Europol staff, law enforcement authorities, EU policy makers, other experts on impact of	**Desk research:** Academic papers, grey literature, Europol's operational support documents **Interviews:** JSPG, Member States Ministries of Interior (political level), COM strategic policy staff, Europol MB, Academia and other experts, NGOs

			external factors (e.g. on Europol's effectiveness. Perceptions about the development of technology for LEA purposes. Perceptions about developments of use of technology for criminal purposes. **Quantitative:** Evolution of the number of stakeholders with which Europol is expected to cooperate and of its areas of activity.	**Survey:** Member States law enforcement authorities, EU agencies and bodies; General public (public consultation)
5	To what extent does Europol make effective and proportionate use of the different **task domains (6 core areas: information management, operational support, strategic analysis, specialised expertise (expert support centres), private sector cooperation, external**	Europol's makes satisfactory and proportionate use of all task domains and tools entrusted to it to achieve its objectives and tasks as set out in its legal mandate. There is clear complementarity between the use made by Europol of its task domains	**Qualitative:** Impact of development of tools and task domains on crime and terrorism. **Opinion-based:** Europol staff views on the use of different powers and tools as set out	**Desk research:** Europol's operational documents, academic research, National information on ENUs and their impact. **Interviews:** JSPG, Member States Ministries of Interior (political level), COM strategic

	cooperation) - and tools (EIS, SIS, EAS, SIENA, Big data processing, system with EPPO) under the current legal framework?	and tools and Member State law enforcement authorities' activities. The mere fact that Europol disposes of certain tasks and tools has already a deterrent effect for criminals and terrorists regardless of its use.	in the legal mandate and likely impact on crime/ deterrent effect. Public and academic experts – on use of Europol of its powers and tools and possible impact on crime / deterrent effect. **<u>Quantitative:</u>** Statistical information on the use and costs of the various tools such as EIS, SIENA, EAS, big data processing, system with EPPO.	policy staff JHA area, Europol MB. **<u>Survey:</u>** Member State law enforcement authorities, General public (public consultation), EU institutions, agencies and bodies.
B	**Efficiency:** How well did Europol use resources relative to the changes achieved?			
	Sub-questions	**Judgment criteria**	**Indicators**	**Data collection tools and method**
6	What are the overall direct and indirect **costs and benefits** of **Europol's core task domains (six core areas: information management, operational support, strategic analysis,**	The overall costs of Europol's activities are proportionate to their impact and outweigh the benefits generated.	**<u>Qualitative:</u>** Resource allocation is proportionate to operations and support provided by Europol.	**<u>Desk research:</u>** Review of grey literature and operational reports, including COM review under Article 68(3) ER, CAARs, Europol Survey on number of staff.

	specialised expertise (expert support centres), private sector cooperation, external cooperation) and how have they evolved since 2017? Are efficiency gains expected or possible in the short or long term?	The activities of Europol do not cause significant costs for Member State law enforcement authorities. The current organization and working methods are highly efficient and there is no scope for savings or room to achieve the same results in a more efficient way. The activities of Europol generate (on balance) efficiencies gains for Member State law enforcement authorities.	**Opinion-based:** Europol staff, EU policy makers on perceived levels of cost and benefits of Europol's activities. Perspective of strengths and gaps or cost-intensiveness. **Quantitative:** Statistics on resources by year and their evolution and employment by the Agency. Allocation of resources per core areas.	**Interviews:** JSPG, Europol MB, Member States Ministries of Interior (political level), ECA. **Survey:** Member State law enforcement authorities and EU agencies and bodies, general public (public consultation). **Case studies:** Review of specific operations and their costs and benefits, collecting deep insights, drawing on good practices.
C	**Relevance:** To what extent do the objectives of the Regulation continue to align with current needs within the EU and among stakeholders?			
	Sub-questions	**Judgment criteria**	**Indicators**	**Data collection tools and method**

7	To what extent do Europol's objectives and activities (core task domains) under its legal framework correspond to the evolving needs within the EU and among affected stakeholders?	Europol's objectives and activities are well aligned with Regulations and corresponding to needs of affected key stakeholders. Europol's activities and objectives are well aligned with the legal framework setting up Europol and Member State needs. Regulatory framework is adapted to evolving needs of the Agency and its stakeholders.	**Qualitative:** Needs of Member States law enforcement authorities, Europol staff, EC, European Parliament, JHA agencies. Coherence of Europol's objectives and activities with Regulation 2016/794 as amended by Regulation 2022/991. Trends of crime and development of criminal activities, broader trends of technology development, needs in terms of data sharing, trends for cooperation with third countries. **Opinion-based:** Perspectives on alignment of Europol's objectives and activities as stated in amended Regulation with evolving needs of affected stakeholders and Europol collaborators.	**Desk research:** Review of grey literature and operational reports, stakeholder reports **Interviews:** JSPG, COM, Member States Ministries of Interior (political level), strategic policy staff JHA area, Europol MB, academia, networks. **Survey:** Member State law enforcement authorities, COM and EU agencies and bodies staff, general public

			Views on needs of adaptation of regulatory framework applicable to Europol **<u>Quantitative:</u>** SOCTA reports	
D	**Coherence:** internal coherence - to what extent Europol various components or interventions achieve together the overall Europol objectives? External coherence - how well different interventions of Europol work with other EU policy interventions, other EU agency interventions or international ones - as well as national/ regional local level interventions?			
	Sub-questions	**Judgment criteria**	**Indicators**	**Data collection tools and method**
8	To what extent are Europol's objectives and activities (core task domains) under its legal framework coherent with other relevant EU policy developments, in the fields of law enforcement cooperation and security, including with ProtectEU, the European Internal Security Strategy?	Europol's objectives and activities as set out under legal framework are coherent and aligned to EU polices related to law enforcement cooperation and security. Europol's objectives and activities as set out under its legal framework created synergies with other EU	**<u>Qualitative:</u>** Evidence that Europol's objectives and activities worked in coherence with other EU law enforcement cooperation and security policies. Evidence or indications of contradictions, synergies and gaps.	**<u>Desk research:</u>** Review of grey literature and operational reports, including COM review under Article 68(3) of the Europol Regulation. **<u>Interviews:</u>** JSPG, COM, COSI, strategic policy staff JHA area, Member States Ministries of Interior (political level), Europol MB.

		policies in the field of law enforcement cooperation and security No evidence of contradictions between Europol legal framework and other EU policies on law enforcement cooperation and security. There was no evidence of overlaps between Europol's legal framework and EU policies on law enforcement cooperation and security.	**Opinion-based:** Stakeholders' views on existence of synergies, gaps, coherence, contradictions and overlaps.	**Survey:** Member States law enforcement authorities and EU agencies and bodies, general publics (public consultation).
E	**EU Added value**			
	Sub-questions	**Judgment criteria**	**Indicators**	**Data collection tools and method**
9	Without Europol, how effectively could Member States conduct and exchange investigations and information at their current scale?	Member States do not have the possibility to carry out investigations and information exchange in a comparable scale and manner without the support of Europol in the current context.	**Qualitative:** Baseline of current scale of exchanges. Evidence on cases or specific requests, activities where Europol	**Desk research:** Review of grey literature and operational reports **Interviews:** JSPG, COM strategic policy staff JHA area, Member States Ministries of

		Member States clearly relied on Europol's activities and knowledge.	had key role in investigation or sharing of knowledge. Evidence on existing Member States practices on investigations and exchanges of information. Absence of indications that Member States could have achieved the same results without Europol's expertise in investigations and knowledge. **Opinion-based:** Stakeholders' perspectives on the ability of Member States to carry out the same investigations and exchanges of information, pointing to clear cases, instances. **Quantitative:** EIS information, use of EAS and SIENA.	Interior (political level), Europol MB, Europol Police Chiefs. **Survey:** Member States law enforcement authorities and EU agencies and bodies, general public (public consultation). **Case studies:** specific cases of cross-border investigations conducted with and without Europol's involvement, understand effectiveness and challenges faced in both scenarios.

ANNEX 8: INVENTORY OF EXISTING INFORMATION SYSTEMS AND TOOLS AT EUROPOL

This inventory provides an overview of Europol's main information systems and tools to support Member States in preventing and combating serious international and organised crime, cybercrime and terrorism.

It is aimed at facilitating navigation through the Agency's operational environment by presenting core systems, information exchange tools, operational support tools and coordination mechanisms.

1. Core Operational Systems

Store, process and analyse operational criminal data shared by Member States

Europol Information System (EIS)

Europol's central criminal information system. It contains information related to suspected and convicted persons, criminal networks and structures, offences and criminal activities, objects used to commit crimes (e.g. vehicles, communication devices, financial accounts).

Data can be inserted into the EIS manually through a specific Europol's web application, or automatically through a data loader solution. Newly inserted data is automatically compared with existing information in the system to identify potential matches.

The EIS user community includes officials in the Member State Europol National Units (ENUs), Member State liaison officers at Europol, as well as Europol officials and seconded national experts (SNEs).

Europol Analysis System (EAS)

Operational information system hosting data contributed by Member States and Third Parties. It supports Europol analysts in their operational and strategic analysis of data provided by Europol's stakeholders and enables information to be managed centrally.

Analysis Projects (APs)

Operational data processed in the EAS is organised in **Analysis Projects**. As intelligence platforms supporting criminal investigations related to specific crime areas, they enable Europol and Member States to collect and analyse operational data, identify criminal networks and links between investigations, support international investigations through analytical products.

They focus on certain crime areas from commodity-based, thematic or regional angles (e.g., drugs trafficking, Islamist terrorism, Italian organised crime).

2. Information Access and Exchange Tools

Exchange operational information and securely access Europol data systems

Secure Information Exchange Network Application (SIENA)

The Agency's main platform for the secure exchange of operational and strategic crime-related information. It enables communication between Europol, EU Member States, EU agencies, Third Parties and international partners with cooperation agreements.

The application allows the exchange of information on three classification levels: EU Confidential (EU-C), EU Restricted (EU-R), and Basic Protection Level (BPL).

SIENA can be used by liaison officers, Europol officials, ENU personnel and other designated law enforcement authorities. Third Parties with whom Europol has cooperation agreements are also connected to SIENA.

Querying Europol Systems (QUEST)

Web service integrated in national system interface(s) of Europol Member States. It allows law enforcement authorities to query Europol data directly from their national interfaces.

It enables searches in the EIS and APs and allows queries concerning persons, firearms, identity documents, means of communication, means of transportation, financial accounts and means of payment.

Large File Exchange

System allowing the secure exchange of large volumes of data that exceed the size limitation of file attachment in SIENA. It is used to exchange large datasets related to criminal investigations, such as digital evidence or extensive operational datasets.

It can also be used for bilateral exchanges of large data volumes.

3. Operational Coordination Mechanisms

Support the coordination of international investigations and operational responses involving multiple Member States.

24/7 Operational Centre

By ensuring continuous operational support for Member States and Europol partners, it monitors operational and non-operational information exchange through SIENA, provides first-level response on a 24/7 basis to law enforcement authorities' requests and supports urgent cross-border investigations.

Joint Cybercrime Action Taskforce (J-CAT)

24/7 permanent taskforce operating from Europol headquarters together with the European Cybercrime Centre (EC3). It coordinates intelligence-led coordinated actions against key cybercrime threats and targets. It also facilitates between law enforcement agencies from different countries.

Governed by a Board composed of at least one senior law enforcement representative per participating agency.

Operational Task Force (OTF)

Established by EU Member States and operational partners to target a High Value Target involved in serious and organised crime or terrorism, it temporarily brings investigators and analysts from the relevant countries to enhance coordination, intelligence sharing and operational cooperation during cross-border cooperation. Europol offers analytical and operational support.

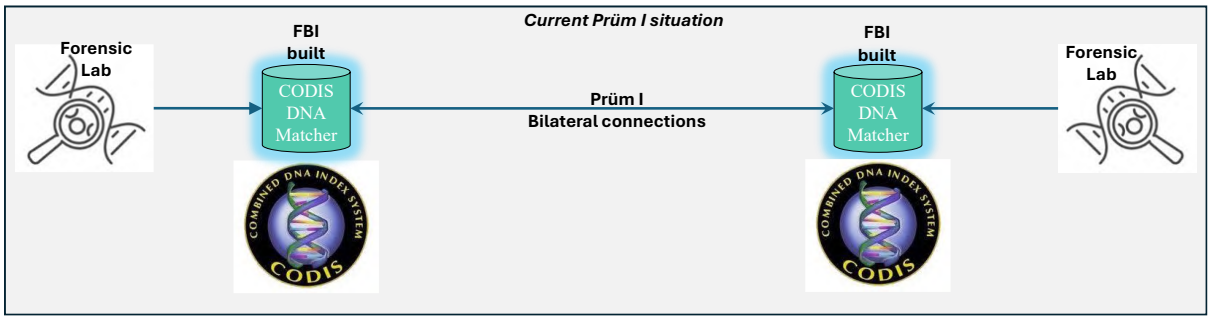
ANNEX 9: DNA MATCHING SERVICE

DNA is currently the most widely used biometric modality in the European Union for the identification of individuals and the resolution of criminal investigations.

Within the EU, DNA profiles are always generated by accredited national forensic laboratories. These certified laboratories analyse DNA samples, either collected from a known individual (typically through a buccal swab) or recovered as biological traces from a crime scene. The analysis involves a series of complex biological, chemical and physical processes that ultimately produce a standardised DNA profile suitable for forensic comparison.

Once generated, each DNA profile is stored in a national DNA database, where it can be compared against other profiles to identify potential matches. Such matches may occur between a crime scene trace and the profile of a known individual, or between crime scene traces originating from different investigations, thereby helping to establish links between criminal cases.

Currently, 23 out of the 27 EU Member States use the **Combined DNA Index System (CODIS)** as the software application for managing national DNA databases and performing DNA profile comparisons. CODIS is owned, developed and maintained by the **Federal Bureau of Investigation (FBI) of the United States**. Under the existing **Prüm framework**, national CODIS systems are interconnected, enabling automated cross-border DNA comparisons between Member States.



While the process of DNA matching itself is computationally straightforward compared to other biometric modalities, it is governed by a set of highly specific and rigorous biological rules that must be applied consistently. Unlike facial recognition or fingerprint matching systems, DNA profile matching does not rely on artificial intelligence or machine learning techniques, but instead on deterministic comparison algorithms based on established forensic standards.

The **Prüm II Regulation[228] and its implementing act[229]** introduce important changes to the DNA profile comparison framework. In particular, DNA profile exchanges will be

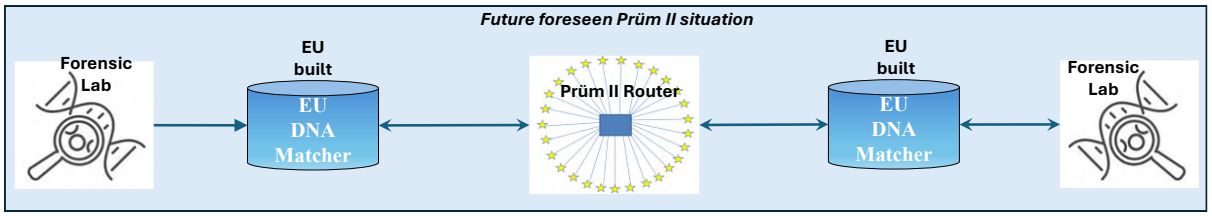
[228] Regulation (EU) 2024/982
[229] [Note to publication colleagues, link to be updated in June when the IA is published with the right reference]

routed through a **centralised technical router operated by eu-LISA**, and updated matching rules will apply. Implementing these changes requires modifications to the CODIS software currently used by Member States. As CODIS is proprietary software owned and maintained by the FBI, such changes can only be carried out by the United States authorities.

This situation creates a structural technological dependency of the EU on a third country for a core component of its law enforcement infrastructure. In the current geopolitical context, reducing such dependencies has become an increasingly important objective for the Union, particularly in sensitive areas related to internal security and law enforcement cooperation.

To address this dependency, the EU could develop, deploy and maintain its own **European DNA matching service** capable of performing the same core functionalities currently provided by CODIS. Such an EU-developed application would implement equivalent DNA profile comparison rules and database management capabilities, while being fully aligned with EU legal and operational requirements. Member States would progressively migrate their existing DNA profiles from CODIS to the new EU system, after which CODIS would no longer be required for national DNA profile database management or cross-border comparisons.

Developing an EU-controlled DNA matching service would enhance the Union's technological sovereignty in a critical area of forensic cooperation, while ensuring full operational continuity for national authorities and supporting the long-term sustainability of the Prüm II framework.



ANNEX 10: IMPACTS OF POLICY OPTIONS

The information presented in this annex aims to enhance transparency and provide further evidence underpinning the conclusions of the impact assessment. The annex should therefore be read in conjunction with the main impact assessment, as it provides the technical background and detailed results that support the overall evaluation of the policy options.

Environmental impact: None, as the options do not involve environmental aspects.

Economic impact: Limited to EU and Member State investment in Europol human and technical resources; no direct effects on private operators or SMEs are expected.

As certain options involve the exchange of personal data, particular attention is given to **fundamental rights**, in line with the EU Charter. Any interference must be **necessary and proportionate** (Articles 51–52), balancing security objectives with protection of personal data (Articles 7–8) and privacy. The options aim to improve law enforcement effectiveness, supporting public security and preventing serious crimes such as human trafficking (Articles 2 and 5 of the Charter).

Data protection is safeguarded by the **Europol Regulation**, the Law Enforcement Directive, and the EU Data Protection Regulation, ensuring legality, necessity, and proportionality of processing. Limitations on rights are targeted, strictly within existing law enforcement mandates. Each option pursues the general interest of EU internal security, and the assessment focuses on **necessity** and **proportionality**.

The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'neutral' (0) and 'negative impact' (-).**Reinforcing Europol's existing model**

1.1 ***Sub policy option 1.1*****: *Strengthened data availability, processing and service***

a. Impact on citizens (+)

This option **protects EU citizens** by enabling Europol to **cross-check and analyse lawfully available data**, allowing **earlier detection of criminal networks**, faster **Member State coordination**, and more **targeted law enforcement**, while focusing on **priority crimes** and preserving **Member State control** and **fundamental rights**.

b. Impact on national authorities (++)

This policy option has a **very positive impact** on national authorities by addressing operational, technical and resource constraints and improving the **returns of cooperation** with Europol. Member States gain:

- **Automated data-loaders**, reducing manual uploads and delays;
- **Systematic cross-checks** by Europol, enhancing intelligence quality;

- **Upgraded systems** (SIENA, EIS, EAS, QUEST/QUEST+), enabling faster and more actionable analysis;
- **Dedicated technical support**, including specialised teams for integration and optimisation;
- J**oint procurement**, reducing costs and promoting interoperability.

Overall, the option improves the **cost–benefit of sharing data**, encourages **systematic engagement**, and strengthens **mutual trust** and **EU-level law enforcement effectiveness**.

c. Impact on fundamental rights

i. Objective of general interest (+)

This option supports the **prevention, detection, and investigation of serious crime and terrorism** by improving the **efficiency, quality, and timeliness of information exchange**. Automated **data-loading** and **proportionate cross-checks** by Europol enhance **intelligence accuracy** and reduce delays and duplication. Upgraded systems (SIENA, EIS, EAS, QUEST/QUEST+) provide **faster queries, stronger analytics, and traceable processing**, while technical support and joint procurement promote **interoperability, data quality, and compliance**. Overall, it fosters a **systematic, accountable, and transparent** use of shared information.

ii. Impact on data protection (0)

Overall, the policy option has a **neutral to slightly positive impact on data protection**.

Necessity

The measures tackle inefficiencies in current cooperation, such as fragmented and manual data-sharing. **Automated data-loaders** ensure that lawfully shareable data are **complete, accurate, and consistently used**. System upgrades and technical support make existing tools **function effectively** and comply with **EU data protection standards**, without changing retention, access rights, or processing purposes. We therefore conclude that the policy option **respects the principle of necessity**.

Proportionality

The option preserves **full Member State control** over shared data, with **purpose limits**. System upgrades improve **architecture, reliability, and safeguards** without changing the legal balance. Overall, measures focus on **enhancing lawful processing** while respecting **existing safeguards and oversight**. We therefore conclude that the policy option **respects the principle of proportionality**.

d. Costs (0)

	Member States	***Europol***
Direct costs		

Expected one-off costs (in million EUR) 1) Data loaders 2) Upgrade of systems and tools	81 (3 per MS) 1) 54 2) 27	61 1) 5 2) 56
Expected yearly recurring costs (in million EUR *per annum*) 1) Data loaders 2) Upgrade of systems and tools	16.2 1) 10.8 2) 5.4	12.2 1) 1 2) 11.2

This option entails upfront investment at both Member State and Europol level, primarily driven by **data loaders as well as system and tools** (including enhance use of interoperability tools). The financial effort reflects a **structural modernisation of the EU law enforcement information architecture**, with medium to long-term savings and operational gains. For more details on the costs of this policy option see Annex 3.

e. Feasibility (+)

Technical feasibility is **high**. The main components, automated data-loaders, interoperability tools and Europol systems (SIENA, EIS, EAS, QUEST/QUEST+), are already operational. The option focuses on **scaling and upgrading existing capabilities**, not creating new infrastructures. Europol's in-house expertise and eu-LISA's experience with large-scale EU systems further reduce implementation risks and support secure, coherent deployment. Where relevant, synergies with eu-LISA's infrastructure, interoperability architecture and technical standards can support secure implementation, ensure consistency across EU information systems and reduce duplication of effort. This institutional ecosystem significantly mitigates implementation risks.

Political feasibility is positive. The option **preserves Member State control** and does not expand Europol's mandate or introduce indiscriminate data transfers. By delivering tangible operational benefits – stronger analytical support and reduced administrative burden – it aligns EU-level improvements with national interests.

Overall, the measure is **feasible from a technical, operational and political perspective**.

f. Impact on digitalisation (++)

This option has a **very positive impact** because it advances the **digital transformation of EU law enforcement** by introducing **automated data-loaders**, enabling **faster, more reliable, and systematic** information exchange. It **automates existing processes**, reduces administrative burden, and supports **near real-time cross-border flow**. **Standardised data models** and guidance foster **interoperability** across Member States, while timely, structured data feeding enhances **analytical capabilities** and **real-time intelligence services**. The infrastructure also lays the foundation for **future digital initiatives**, embedding the **'digital by default' principle** without creating new legal obligations.

1.2 <u>Policy option 1.2</u>: enhanced mitigating measures to address the obstacles of data subject categorisation

a. Impact on citizens (0)

This policy option has a neutral impact on citizens (0). It does not constitute any significant changes, as the obligation to carry out the categorisation of data subjects remains unchanged. Instead, the measures of this option aim at improving the situation for national authorities by facilitating the overall process.

b. Impact on national authorities (+)

The option has a positive impact on national authorities as it would result in more streamlined processing of complex and large datasets. Due to the detailed internal guidance and tools (checklists, templates, standard scenarios) that would be developed as part of this option, there would be reduced operational delays and fewer inconsistencies, resulting in the overall positive impact on national authorities. Greater legal certainty and clarity in applying DSC rules would also reduce the risk of errors and subsequent corrective actions.

c. Impact on fundamental rights (0)

i. Objective of general interest (+)

This option makes a positive contribution to an objective of general interest (+), as it constitutes a measure to facilitate the overall fight against serious and organised crime. Improving and harmonising the practical application of the rules governing data subject categorisation and the subsequent improvement would lead to more consistent and reliable data processing, facilitating the work of both national authorities and Europol, resulting in faster operational results and investigations.

ii. Impact on data protection (0)

Necessity

The flaws and obstacles of the current DSC framework have been highlighted both by the national authorities of the Member States as well as by the Commission, as underlined by the report pursuant to article 68(3) of the ER[230], resulting in the necessity for a change to such rules and the operational capabilities.

By utilising current tools and methodologies to reduce errors and inconsistencies in data categorisation, the overall level of data protection is maintained and strengthened through improved compliance and consistency. We therefore conclude that the policy option **respects the principle of necessity**.

[230] COM(2025) 752 final, 11.12.2025.

Proportionality

The policy option of addressing the obstacles of DSC by introducing mitigation measures is fully proportionate as it would aim to harmonise and streamline currently existing rules rather than introduce new ones. Standardising the process of DSC while increasing the legal certainty and simultaneously making it more efficient and less resource-intensive, demonstrates the proportionality of this option. No new categories of data, new processing purposes or expanded access rights are introduced. We therefore conclude that the policy option **respects the principle of proportionality**.

d. Cost (+)

The overall cost of this option is difficult to estimate. The option will require small initial investments related to the development of internal guidance, tools and training materials. In the long-term, however, the initial cost of labour needs would be offset by the overall benefit of clarifying and improving the framework on DSC, reducing inefficiencies and corrective workload.

e. Feasibility (++)

This policy option has very positive feasibility as it would be easily put into place. The *technical feasibility* would not require developing an entirely new framework for DSC but rather improving and further developing a set of rules already in place.

The *political feasibility* would be equally as positive (++) as national authorities have underlined the need for further clarifications and guidelines, as well as the necessity to reform the overall process of DSC. This policy option should therefore face little to no political opposition.

f. Impact on digitalisation (0)

The option has an overall neutral impact on digitalisation. While it relies on existing digital infrastructures, it does not fundamentally transform the digital architecture of the process of data subject categorisation. Subsequently putting in place mitigating measures to address the obstacles of DSC serves as an enabler for Europol to process and analyse data rather than being a driver of structural change. Meaning that Europol's overall usage of data would be (further) consolidated, which has no impact on digitalisation as such.

1.3 Policy option 1.3 - Measure 1 on reinforced Europol's support to the EPPO

EPPO Support Unit: a reinforced, dedicated unit within Europol's Financial and Economic Crime Centre (EFECC), composed of specialised staff assigned exclusively to EPPO-related cases, replacing and reinforcing the current small team handling these. The organisation of the unit would not change compared to what is currently in place with the current small team except in terms of staff, which would however grow significantly. The unit's staff will need to be specialised in VAT fraud, customs fraud, excise fraud, and trade-based money laundering, and should have familiarity with the complex multi-criminal behaviours of modern organised crime groups (MTIC schemes). Four different

types of support tasks would be handled by the unit: cross-checks of EPPO data against Europol database (hit/no-hit), digital forensics (in particular making information in seized devices available for operation analysis), operational analysis (making sense of data gathered in EPPO cases), and operational support (e.g. assets tracing, preparatory activities for action days, manning virtual command posts). The Europol-EPPO Working Arrangement would be updated accordingly.

a. Impact on citizens (+)

This measure would reinforce the protection of EU citizens against the crimes for which the EPPO is competent and the criminal actors involved. Therefore, this measure has a positive impact on citizens.

b. Impact on national authorities (+)

Europol's reinforced support to the EPPO will help further extract criminal proceeds from criminal actors. Therefore, this measure has a **positive impact on national authorities (+).**

c. Impact on fundamental rights (+)

This measure would have a positive impact on fundamental rights insofar as it would ultimately help strengthen the EU Member States' statehood against criminal threats, prompting Member States' concrete ability to respect, promote and fulfil human rights under international and EU law.

i. Objective of general interest (+)

This measure makes a **positive contribution to an objective of general interest (+)**, namely the protection of the financial interests of the EU, by allowing the EPPO to effectively carry out its mission vis-a-vis sharply increasing need for support from Europol.

ii. Data protection (0)

Necessity and proportionality

The current Europol staff allocated to support the EPPO (8-9 officers) is not sufficient. This measure is necessary to meet the minimum level of the EPPO's sharply increasingly needs and thus allow it to effectively protect the financial interests of the EU. It does not interfere with current data protection levels. Therefore, this policy measure **respects the principles of necessity and proportionality**.

d. Costs (+)

	Member States activities	***EU activities***
Direct costs		

Expected one-off costs (in million EUR)	0	0
Expected yearly recurring costs (in million EUR)	0	10

One-off costs for Member States are negligible, as the measure focuses on establishing new Europol-level capacities, without requiring structural changes, staff contributions, or procedural adaptations at national level. Recurrent costs arise mainly at Europol, reflecting the long-term employment of specialised officers in the dedicated EPPO Support Team, responsible for operational analysis, cross-checks, and digital forensics, with an average annual cost of approximately EUR 10 million.

e. Feasibility (+)

Technical feasibility

The measure is legally feasible. Establishing the EPPO Support Unit at Europol would not alter the respective mandates or the fundamental nature of the relationship between Europol and the EPPO. It would not require amending the Europol Regulation. Amending the Europol-EPPO Working Arrangement would suffice. From an organisational perspective, the measure would build on existing organisational and technological set-ups (e.g. EFECC, JIT model, case-handling processes), but would require enhanced operational capacity in terms of staff (e.g. capability to support investigations and run analytical tasks, expertise in defined areas [VAT fraud, customs fraud, MTIC]). For this reason, the option is **technically feasible (++).**

Political feasibility

The consultation activities have revealed that both Europol and the EPPO would fully support this measure,[231] while Member States would widely support it[232]. However, several Member States have also emphasised their preference that Europol's support remain essentially focused on the operational needs of the Member States[233]. Overall, the measure is **politically feasible (+).**

f. Impact on digitalisation (0)

This measure would have no to positive impacts on digitalisation depending on whether implementation maintains the current level or increases the digital delivery of services.

[231] Interview, focus groups, targeted survey with agencies.
[232] The responses to the targeted survey for the EU Member States' national law enforcement authorities show support for the update of the working arrangement
[233] As discussed in the COSI meeting of February 2026.

1.4 <u>Policy option 1.3</u> - Measures 2 and 3 for a strengthened continuum of EU-level support to law enforcement cooperation through Europol and judicial cooperation through Eurojust

a. Impact on citizens (+)

These measures would overall reinforce the protection of EU citizens against organised crime, albeit moderately.

b. Impact on national authorities (+)

These measures would overall reinforce the information at disposal of Europol and Eurojust and thus the support they can provide to national authorities, albeit moderately. The national authorities of EU Member States would be able to continue relying on SIRIUS' knowledge and expertise to successfully obtain critical electronic evidence for criminal investigations and prosecutions, namely in a permanent manner.

c. Impact on fundamental rights (+)

These measures would have a positive impact on fundamental rights insofar as it would ultimately help strengthen the EU Member States' statehood against criminal threats, prompting Member States' concrete ability to respect, promote and fulfil human rights under international and EU law.

i. Objective of general interest (+)

These measures make a positive contribution to an objective of general interest (+), namely the EU-level fight against organised crime and cybercrime, by strengthening the continuum of EU-level support through Europol and judicial cooperation through Eurojust.

ii. Data protection (0)

Necessity and proportionality

These measures are necessary to strengthen the continuum of EU-level support through Europol and judicial cooperation through Eurojust. Upgrading the existing hit/no-hit mechanism through the introduction of automated processes is necessary to improve indirect information exchange between Europol and Eurojust. Introducing Institutionalising the mission of the SIRIUS project within the Europol Regulation is necessary to ensure the long-term financial sustainability and permanent support for the national authorities of the EU Member States according to their needs. Therefore, these measures **respect the principles of necessity and proportionality**.

d. Costs (+)

	Member States activities	***EU activities***
Direct costs		

Expected one-off costs (in million EUR)	0	2
Expected yearly recurring costs (in million EUR)	0	1

One-off and recurring costs for Member States are expected to be negligible, as the measures focus on Europol–Eurojust cooperation and build on existing infrastructure, workflows, and personnel. Costs at EU level reflect Europol and Eurojust staffing for the SIRIUS project and the hit/no-hit mechanism, with modest adjustments for institutionalisation and light automation, generating efficiency gains by reducing manual exchanges and improving operational timeliness.

e. Feasibility (+)

Technical feasibility

From a legal perspective, the institutionalisation of SIRIUS would require amending the Europol and Eurojust Regulations regarding their tasks. Article 4 of the Europol Regulation already provides a broad mandate for Europol to support Member States through expertise, training, operational coordination and facilitation of cooperation with private parties. A legislative clarification explicitly mandating Europol to provide structured support on cross-border access to electronic evidence, including cooperation with Eurojust, service providers and third countries, would provide legal certainty, stable governance and budgetary predictability. For the hit/no-hit automation component, both Regulations foresee indirect access to information on a hit/no-hit basis. The current limitations are related to implementation modalities. From a technical perspective, feasibility remains strong.

Political feasibility

From a political perspective, feasibility is high. The SIRIUS EU Electronic Evidence Situation Report 2024 confirms sustained and growing operational demand for EU-level support in accessing electronic evidence.[234] In 2023 alone, competent authorities submitted 266,855 cross-border data disclosure requests to major online service providers, representing a 22% increase compared to 2022, demonstrating the scale and structural nature of demand.[235] Feedback collected in the 2024 report from law enforcement, judicial authorities and service providers highlights the value of centralised expertise, Single Points of Contact (SPoCs) and structured dialogue with private companies.[236] Service providers also emphasised the importance of predictable engagement and harmonised practices, indicating that institutionalisation would enhance

[234] Europol (2025) SIRIUS Electronic Evidence Situation Report 2024.

[235] Europol (2025) SIRIUS EU Electronic Evidence Situation Report 2024 – Factsheets (Law Enforcement, Judicial Authorities, Service Providers).

[236] ibid.

legal certainty rather than create new burdens.[237] These stakeholder views demonstrate broad operational acceptance and support across law enforcement, judiciary and private sector actors, reinforcing the political feasibility of embedding SIRIUS permanently within the Europol and Eurojust mandates.

f. Impact on digitalisation (0)

This measure would have no to positive impacts on digitalisation depending on whether implementation maintains the current level or increases the digital delivery of services.

1.5 Policy option 1.4: Europol digital platforms embedded in national investigations

a. Impact on citizens (++)

This option has a **very positive impact on citizens** by reducing the risk of **undetected cross-border criminal links**. Integrating national **CMS with Europol platforms** and requiring targeted consultation in serious cases embeds checks into everyday workflows, enabling **earlier detection**, reducing blind spots, and improving **Member State coordination**, thereby enhancing overall **citizen security**.

b. Impact on national authorities (+)

This option benefits **national authorities** by embedding Europol support directly into **CMS workflows**, allowing investigators to consult platforms and receive **analytical feedback** within their national environment. Targeted consultation in serious cross-border cases ensures EU-level information is systematically used, preventing missed links and supporting early de-confliction. **National authorities retain full control** while gaining **enhanced situational awareness** and more consistent analytical support.

c. Impact on fundamental rights

i. Objective of general interest (++)

This option makes a **strong positive contribution to an objective of general interest, i.e.** the **prevention and combating of serious crime and terrorism,** by embedding Europol platforms into national workflows and requiring targeted consultation in cross-border cases, ensuring EU-level information is systematically used, reducing fragmentation, closing information gaps, and strengthening **early detection of criminal networks**.

ii. Data protection (0)

Necessity

The integration of national **CMS with Europol systems** improves workflows and interfaces without creating new data categories, access rights, or processing purposes. A targeted obligation to systematically consult **EIS** in serious cross-border cases addresses

[237] Europol (2025) *SIRIUS EU Electronic Evidence Situation Report 2024 – Factsheets (Law Enforcement, Judicial Authorities, Service Providers).*

operational gaps, ensuring lawfully available information is effectively used. By embedding consultation as a **structured, proportionate step**, the measure reduces blind spots, prevents information gaps, and ensures existing **data-sharing mechanisms** function as intended. We therefore conclude that the policy option **respects the principle of necessity**.

Proportionality

This option does not create new data categories, databases, or purposes; it **structures existing lawful access** to Europol systems, notably **EIS**, within national CMS. A targeted obligation to consult EIS in serious cross-border cases ensures that lawfully available data is **consistently and effectively used**, without expanding Europol's mandate. Embedded consultation reduces missed links and fragmentation while preserving **national control, purpose limitation, and data ownership**, ensuring interference with **data protection rights** is proportionate.

We therefore conclude that the policy option **respects the principle of proportionality**.

d. Costs (0)

	Member States	***Europol***
Direct costs		
Expected one-off costs (in million EUR)	105	50
Expected yearly recurring costs (in million EUR *per annum*)	20	8

One-off costs for Member States (EUR 105 million) cover new criminal information strategies, updates to case management systems, integration with UMF standards, and training, with recurring costs (EUR 20 million/year) for ongoing maintenance. Europol one-off costs (EUR 50 million) include upgrades to data ingestion, scaling of databases, and support to Member States, with recurring costs (EUR 8 million/year) for continued operational and integration support.

Technical feasibility

Integrating national **CMS with Europol systems** requires secure APIs, harmonised data models, workflow adjustments, and increased capacity, but builds on existing **SIENA connectivity** rather than creating a new digital ecosystem. Implementation will need substantial **EU and national resources**, including development, testing, training, and change management, with **Europol providing central support** through toolkits, reference architectures, and on-site assistance. Systematic consultation is technically feasible only if **Europol systems are robust, scalable, and able to handle increased queries** while delivering timely responses.

For this reason, the option is **technically feasible (+) only in conjunction with Policy Option 1.1**, which upgrades Europol's ICT infrastructure, performance and service delivery. Without Option 1.1, embedding systematic consultation into national workflows would risk system overload, latency and reduced reliability, making overall feasibility **negative (–)**.

Political feasibility

Political feasibility is **ambitious**, as embedding Europol systems into national CMS and introducing systematic consultation represents a major shift for Member States. While benefits are clear, **faster detection, improved situational awareness, and better analytical support**, authorities may resist changing established workflows. Feasibility is higher with **phased implementation**, pilot projects, peer exchanges, and strong **Europol support** to build trust. Rapid, large-scale deployment without engagement and resources is unlikely to succeed. Overall, the option is **politically feasible but facing significant obstacles (-).**

e. Impact on digitalisation (+)

This option advances the **digitalisation of EU law enforcement** by integrating national **CMS with Europol systems** and enabling **systematic consultation** of EIS/EAS. It replaces **manual, ad hoc processes** with **automated workflow checks**, standardises information exchange, and delivers **timely, actionable analytical outputs**, improving usability, automation, and effectiveness of existing systems while reinforcing the **'digital by default' principle'**.

1. Designing a new model for Europol

2.1 Policy option 2.1: Europol as an operational service provider and information hub

a. Impact on citizens (+)

Overall, this policy option has a **positive impact on citizens (+)**, by enhancing the EU's capacity to prevent and combat serious crime while preserving **Member State control**. Europol, when authorised, could query national databases under **Prüm II** (DNA, fingerprints, facial images), police indexes, and vehicle records, acting strictly on behalf of Member States. In **time-critical or large-scale cases**, Europol's technical and forensic support enables faster cross-border link detection. An **EU DNA matching service** would strengthen forensic cooperation, reduce reliance on third-country tools, and improve the **speed and reliability** of cross-border investigations.

b. Impact on national authorities (++)

This option strongly benefits **national authorities**, especially investigators handling complex or cross-border cases, by allowing Europol, strictly **on behalf of and with explicit authorization**, to query national databases under **Prüm II**. Authorities gain **faster handling of biometric and non-biometric queries**, **technical and forensic support** in high-volume cases, and **improved analytical coherence** across jurisdictions. Real-time alerts and subscription-based notifications reduce fragmentation and ensure that relevant

developments are not missed, without creating automatic data transfers. Political acceptability relies on **strict safeguards, authorisation, and clear governance**.

The optional **EU DNA matching service** would provide shared forensic capabilities, reduce dependency on third-country tools and align with **Prüm II standards**. Member States would benefit from **faster adaptation to evolving requirements**, **operational continuity**, and **support for smaller forensic authorities**, while maintaining **national ownership of data and investigative decisions**. The service strengthens **strategic autonomy** and **technical resilience** in cross-border investigations.

c. Impact on fundamental rights

i. Objective of general interest (+)

This option makes a **positive contribution to an objective of general interest (+)**, namely the prevention and combating of serious crime and terrorism. By combining **authorised Europol access** to national data under **Prüm II**, improved system interoperability, and shared services such as a potential **EU DNA matching service**, this option strengthens the **speed, coherence, and reliability** of cross-border investigations. It reduces fragmentation, enables **earlier detection of cross-system links**, and enhances **forensic cooperation** in complex or time-critical cases, while Europol acts strictly within its mandate and on **Member State authorisation**, without centralising data. Overall, it reinforces **EU internal security** and delivers clear **EU added value**.

ii. Impact on data protection (0)

Necessity

Allowing Europol, with explicit **Member State authorisation**, to query national databases under **EU frameworks** addresses operational gaps that currently cause delays and blind spots. Anchored in the **Prüm II hit/no-hit architecture** and maintaining full **national control**, Europol acts as a **technical and analytical service provider** without new data categories or autonomous access rights, ensuring more effective cross-border cooperation, particularly in **complex or time-critical cases**.

A shared **EU DNA matching service** enhances **operational resilience**, aligns with evolving **Prüm II standards**, and reduces reliance on third-country tools. Developed with Member States and forensic authorities, it is **optional and fully governed by Member States**, providing a common solution for lawfully collected data while preventing fragmentation and ensuring consistent application of **EU data protection standards**. Both measures are **necessary and targeted**, addressing identified operational gaps without expanding Europol's mandate or data scope.

This policy option **passes the necessity test**.

Proportionality

Europol access strictly limited to **Prüm II** and under **Member State authorisation** is proportionate, preserving the **hit/no-hit architecture, national control, case-based use,**

and data ownership, without expanding data categories or retention. This supports cross-border investigations without exceeding what is necessary, while any access beyond Prüm II is **not proportionate** and excluded from option comparisons.

A shared **EU DNA matching service**, developed with Member States and aligned with Prüm II, is proportionate. It does **not create new data categories**, remains **optional and Member State–governed**, and preserves **decentralised storage and ownership**, providing common infrastructure for lawfully exchanged DNA data. Its benefits – enhanced effectiveness and **EU strategic autonomy** – outweigh the limited, controlled impact on data processing. We therefore conclude that the option **respects the principle of proportionality**.

d. Costs (+/--)

	Member States	***Europol***
Direct costs		
Expected one-off costs (in million EUR) 1) Access to national databases 2) DNA matcher	1.35 (0.05 per MS) 1) 0 2) 1.35	11 1) 6 2) 5
Expected yearly recurring costs (in million EUR *per annum*) 1) Access to national databases 2) DNA matcher	0.3 1) 0 2) 0.3	5.3* 1) 4.3 2) 1

Under the Prüm-based approach, Member States' costs remain negligible, with only limited technical adjustments and a small one-off cost (around EUR 0.05 million per Member State). Europol bears moderate initial and limited recurring costs for additional staff, reinforced data management and minor system upgrades, including the EU DNA matcher. While EU-level expenditure increases, overall Union costs are expected to decrease over time through economies of scale and reduced reliance on third-country solutions.

e. Feasibility (+)

Technical feasibility

Technical feasibility is high for **Prüm II–based authorised access**, as the necessary hit/no-hit infrastructure, secure channels, and biometric matching are already in place, requiring mainly workflow and configuration adjustments. A shared **EU DNA matching service** is more complex but feasible, building on existing forensic standards, technologies,

and Prüm frameworks, and requiring robust **security, governance, and Member State cooperation**. With phased implementation, both measures are technically feasible, giving an overall **positive feasibility assessment (+)**.

Political feasibility

The policy option in politically feasible (+). **Prüm II-based authorised access** is challenging, as it shifts Europol's role to querying Member State data, but is acceptable when Europol acts **strictly on Member State request**. Any access beyond Prüm II would likely face strong opposition. The **EU DNA matching service** is politically feasible, as it enhances **strategic autonomy**, reduces reliance on third-country tools, and remains **optional and Member State-governed**.

f. Impact on digitalisation (0)

The option has a **neutral impact on digitalisation**, relying on existing infrastructures like **Prüm II** and forensic technologies without fundamentally transforming EU law enforcement's digital architecture. **Prüm II access** builds on established frameworks, and the optional **EU DNA matching service** consolidates existing capabilities. Digital tools primarily **enable operational support** rather than driving structural digital transformation.

2.2 ***Policy option 2.2: Simplified rules to reduce the administrative burden of data subject categorisation***

a. Impact on citizens (+)

As this policy option would allow both Europol and the EU Member States to use data more effectively and consistently, there would be a direct, positive impact on Europol's ability to fight serious and organised crime and terrorism. By reducing operational delays and increasing legal clarity, investigations could progress more efficiently, leading to a positive impact on citizens and strengthening overall security.

b. Impact on national authorities (++)

The option would significantly change and simplify the process of Member States sharing data. It would lead to harmonisation of rules applicable to Member States and Europol alike, by aligning the Europol Regulation with the Law Enforcement Directive (LED) and the EU Data Protection Regulation (EUDPR), resulting in clearer and more coherent rules for national authorities.

In addition, the overall harmonisation would lead to a decrease in bureaucracy, constituting another very positive impact on national authorities. Greater legal certainty would also reduce the risk of divergent interpretations and corrective actions.

c. Impact on fundamental rights (+)

i. Objective of general interest (+)

This policy option would have a clear positive impact as regards the objective of general interest. A simplified and harmonised framework for data subject categorisation would enhance Europol's operational effectiveness positively contributes to the ability of Europol to fight against serious and organised crime and terrorism by lessening operational burden on Europol and eliminating operational delays currently faced.

ii. Impact on data protection (-)

Necessity

This policy option proves to be of a high necessity as it would positively impact the way data would be analysed and used by Europol. Whereas currently data may remain underused due to the complex framework governing data subject categorisation, the option would allow for data to be processed and analysed more efficiently, **within a clearer and legally aligned structure**. This ensures that data already lawfully collected can be effectively used for its intended law enforcement purpose. We therefore conclude that the policy option **respects the principle of necessity**.

Proportionality

The option is proportionate in that it does not introduce new categories of data, new processing purposes, or expanded access rights. However, the removal and simplification of the Data Subject Categorisation (DSC) entail a **moderate negative impact on data protection**, as some of the procedural safeguards that previously limited operational processing are reduced. The measure aligns existing rules with the LED and the EUDPR and reduces procedural constraints, thereby enhancing operational coherence and effectiveness. By maintaining the core safeguards and limiting the scope of processing to operationally necessary cases, the option seeks an appropriate balance between efficiency and fundamental rights. We therefore conclude that, while there is a negative impact on data protection, the **policy option remains proportionate** in relation to the objectives pursued.

d. Cost (++)

Even though the policy option would significantly improve Europol's operational flexibility and capacity to process information, it would not require substantial initial investment, as it primarily concerns legislative alignment and simplification. Moreover, this policy option would likely free up resources that are currently deployed to specifically engage in the burdensome procedure of data subject categorisation under the current framework.

Administrative savings and efficiency gains are therefore expected, justifying the very positive cost assessment.

e. Feasibility (+)

The *technical feasibility* of this option is to be assessed as very positive (++), as it would not require substantial changes to be put in place or require the development of an entirely new legal framework for DSC. Instead, the framework would be aligned to that of the LED and the EUDPR.

The alignment with already existing legislation would constitute a positive assessment as regards *political feasibility* (+). Overall, this harmonisation would be well-received by Europol and the Member States aligned, as underlined by the recent report under article 68(3) of the ER and further consultation of Member States' experts at technical level. However, as this option could potentially offset complexities as regards data ownership and sovereignty, the impact is assessed only as positive and not as very positive.

f. Impact on digitalisation (0)

The option has an overall neutral impact on digitalisation. By aligning existing legal frameworks and procedures, the digital architecture of the process of data subject categorisation is not fundamentally transformed. Subsequently address the obstacles of DSC serves as an enabler for Europol to process and analyse data rather than being a driver of structural change. Meaning that Europol's overall usage of data would be (further) consolidated, which has no impact on digitalisation as such.

2.3 *Policy option 2.3: Europol as structural provider of information, analytical support and capacities to the EPPO*

a. Impact on citizens (++)

The positive impacts on citizens mentioned for policy option 1 would increase thanks to efficiency gains deriving from the introduction of both hierarchical arrangements and direct information exchange between Europol and EPPO. Citizens would also benefit indirectly from Europol having access to further information stored by the EPPO.

b. Impact on national authorities (++)

The positive impacts on national authorities mentioned for policy option 1 would increase thanks to efficiency gains deriving from the introduction of both hierarchical arrangements and direct information exchange between Europol and EPPO. Law enforcement authorities would also benefit indirectly from Europol having access to further information stored by the EPPO, as this would strengthen Europol's support and coordination abilities.

c. Impact on fundamental rights (++)

This measure would have a very positive impact on fundamental rights insofar as it would ultimately help strengthen the EU Member States' statehood against criminal threats in an efficient manner, prompting Member States' concrete ability to respect, promote and fulfil human rights under international and EU law.

i. Objective of general interest (++)

This measure makes a very positive contribution to an objective of general interest (+), namely the protection of the financial interests of the EU, by allowing the EPPO to effectively and efficiently carry out its mission. The same goes for the EU-level fight against serious and organised crime, cybercrime and terrorism, by allowing Europol to develop specialised skills and have access to a huge amount of relevant information to ultimately more effectively support the Member States.

ii. Impact on data protection (0)

Necessity and proportionality

This measure is necessary to efficiently meet the EPPO's sharply increasingly needs and allow it to maximally protect the financial interests of the EU. It does not interfere with current data protection levels. Therefore, this policy measure **respects the principles of necessity and proportionality**.

d. Costs (++)

	Member States activities	***EU activities***
Direct costs		
Expected one-off costs (in million EUR)	0	0
Expected yearly recurring costs (in million EUR)	0	11.1

One-off and recurring costs for Member States are **negligible**, as the measure operates at EU level and does not require national staff contributions or operational expenditure. For Europol, no separate start-up costs are identified, since onboarding and infrastructure needs are already captured in the average annual staff cost methodology. Recurrent costs stem mainly from establishing a **dedicated EPPO Support Team** (around **EUR 10.1 million annually**) and additional permanent cooperation mechanisms (less than **EUR 1 million per year**).

e. Feasibility (+)

Technical feasibility

The measure is legally feasible. Besides establishing the EPPO Support Unit, which was analysed for policy option 1, turning Europol into a structural provider of information, analytical support and capacities to the EPPO would require amending the Europol Regulation regarding Europol's tasks. Introducing the possibility for hierarchical arrangements and direct information exchange between Europol and EPPO when information falls within the EPPO's competence would also require amending the Europol Regulation regarding relations between Europol and EPPO.

Political feasibility

The consultation activities have revealed that the EPPO would fully support this measure,[238] while both Europol and several Member States remain reluctant toward introducing the possibility for information exchanges in derogation from the "data ownership principle"[239]. Overall, the measure remains **politically feasible, albeit with difficulties.**

f. Impact on digitalisation (0)

This measure would have no to positive impacts on digitalisation depending on whether implementation maintains the current level or increases the digital delivery of services.

2.4 *Policy option 2.4: EU Police Cloud and Europol support offices*

a. Impact on citizens (+)

The continued rise of **digitally enabled and AI-facilitated crime**, combined with increased cross-border mobility, has led to a more diverse and complex threat landscape. Criminal activities increasingly span EU internal borders and affect citizens both directly and indirectly. This trend is expected to intensify as a growing share of citizens' daily activities takes place in **digital environments**.

Ensuring a safer physical and online environment therefore requires **enhanced cross-border cooperation**, improved information exchange among Member States, and analytical capacities capable of processing large and complex datasets. The EU Police Cloud would support the deployment of interoperable digital investigative tools and scalable processing capabilities, enabling law enforcement authorities to respond more effectively to evolving forms of criminality. Overall, the initiative is expected to **strengthen EU internal security** by supporting law enforcement adaptation to the digital transformation of crime, thereby delivering **tangible benefits for citizens** in terms of safer physical and online environments.

By strengthening the operational link between Europol and the Member States, through reinforced Europol National Units complemented by **Europol Support Offices**, this measure would establish a more integrated, efficient and operationally driven model of cross-border law-enforcement cooperation. It is expected to deliver tangible security outcomes for citizens, including more effective disruption of cross-border criminal networks, earlier detection of cross-border dimensions in criminal investigations, faster operational responses, and improved coordination of operational and investigative

[238] As stated by the EPPO in the interview carried out by ICF in the context of the study supporting the evaluation and impact assessment of the Europol Regulation, as well as during the third workshop on the future of Europol and in its Note to DG HOME on improving the cooperation between the EPPO and Europol.

[239] As stated by Europol, during the focus groups carried out in the context of the study supporting the evaluation and impact assessment of the Europol Regulation, and by Member States during the fourth workshop on the future of Europol and during the COSI meeting of February 2026.

activities. Over time, this enhanced effectiveness is likely to contribute to a higher level of security within the Union and to reinforce citizens' trust in the EU's capacity to combat serious and organised crime.

b. Impact on national authorities (++)

The EU Police Cloud would provide criminal investigators across the Union with **scalable storage and on-demand computing capacity**, enabling them to manage expanding datasets and peak workloads more effectively. National authorities would benefit from enhanced analytical tools, including AI-supported pattern detection, network and multimedia analysis, and decryption capabilities. These functionalities would support more precise and near real-time data processing, thereby strengthening investigative and crime-prevention capacities.

The initiative would also foster **secure and trust-based cross-border information sharing**. Through harmonised authentication mechanisms and common security standards across Member States, the Police Cloud would offer a unified environment for joint analysis and cooperation. National authorities would retain control over their data throughout its lifecycle, while benefiting from reduced fragmentation and improved interoperability, thus reinforcing mutual trust and operational cooperation.

By enabling the processing of sensitive law enforcement data within a **sovereign European framework**, the transition would contribute to resilience and strategic autonomy. Moving beyond constraints linked to traditional infrastructure would facilitate more efficient data handling and timely operational responses, in line with EU digital sovereignty objectives. Overall, the EU Police Cloud is expected to **enhance operational effectiveness, efficiency and cooperation** among national authorities, supporting strategic law enforcement objectives at Union level.

Europol Support Offices would have a significant operational impact on national law-enforcement authorities. They would provide more systematic and easier access to Europol's analytical, operational, and strategic products, while reducing administrative and coordination burdens through locally embedded expertise familiar with both national procedures and Europol systems. The offices would also strengthen trust and mutual understanding between national services and Europol and support capacity-building through specialised training. Evidence shows that Europol support is often mobilised late in investigations, limiting its impact; these Europol support offices would facilitate earlier engagement, improve uptake of Europol products in national proceedings, and, in the medium term, increase operational efficiency while reducing duplication of efforts.

c. Impact on fundamental rights (+)

i. Objective of general interest (+)

The proposal aligns firmly with the EU's overarching interest in promoting security, peace, and the well-being of citizens through a unified law enforcement framework. In supporting Europol's capabilities, the measure seeks to uphold the collective security interests of Member States, ensuring a harmonised approach to combating serious crime.

ii. Impact on data protection (0)

Necessity

The EU Police Cloud would provide the **scalable storage and processing infrastructure** required to support an expanding range of EU criminal information-sharing and analytical tools. It would enable seamless deployment within national environments and ensure a **high and harmonised level of security**, notably through an EU Digital Police identity framework.

The initiative would **not introduce new personal data or new processing operations**, but would serve as the secure technical backbone for existing and future applications requiring significant computing capacity.

Its necessity arises from the need to process **large, complex and cross-border datasets** that cannot be efficiently handled through decentralised infrastructures alone. Certain joint analytical and communication-based applications inherently require centralised capacity due to volume and operational constraints. Joint cross-border analysis of information shared by Member States, including extensions of JOAC and Europol Analytical Projects, requires **centralised storage and processing**, as the data volumes involved exceed the practical transfer capacities between national data centres. Similarly, communication-based tools such as SIENA, the Large File Exchange (LFE) system, and multilateral operational cooperation mechanisms rely on **central processing infrastructure** to function effectively.

The EU Police Cloud is therefore considered **a necessary enabling measure** to maintain effective and secure EU law enforcement cooperation in the digital environment.

Proportionality

The EU Police Cloud being only a technical platform for hosting law enforcement applications does not entail *per se* any possible consequence on the persons' rights and freedom. Such hosted data processing being however susceptible by the size and the processing power to augment the risks of potential infringements, EU police cloud will accordingly provide by default build-in safeguards ensuring that *a first unconditional line of guarantees* will be available to limit the hosted application to essential purposes in law enforcement: along with harmonized digital police environment, will a common police digital ID scheme, based on EU Digital Identity with insurance level high be the ground stone for insuring traceability, accountability and strong role-based access to such sensitive investigative data and to the corresponding tools.

In that way will the EU Police Cloud *contribute to* safeguarding individual privacy rights for all potential storage and processing of data while maximising operational efficacy. The approach ensures a balanced application of processing power without overextending the access to or usage of personal data.

d. Cost (0)

	Member States	***Europol***
Direct costs		
Expected one-off costs (in million EUR)	***67,5***	***145.8***
- *EU Police Cloud*	- *13,5*	- *143.3*
- *EU Police Digital ID*	- *54*	- *2,5*
- *Europol Support offices*	- *0*	- *0*
Expected yearly recurring costs (in million EUR)	***11,4***	***46.8***
- *EU Police Cloud*	- *0,6*	- *39.8*
- *EU Police Digital ID*	- *10,8*	- *0,5*
- *Europol Support offices*	- *0*	- *6,5*

The initial investment costs associated with the deployment of the EU Digital Police Cloud are substantial, encompassing infrastructure development, data migration, and ongoing system management. Nevertheless, these investments are counterbalanced by long-term savings arising from enhanced processing efficiencies and reduced overhead linked to disparate national law enforcement systems.

A modest Europol support office would generate **approximately EUR 400,000 to EUR 650,000 per year**, covering staff costs, secure IT connectivity, equipment and limited coordination travel. Under a rollout of five to ten antenna offices, total annual EU-level costs would range between **EUR 2 million and EUR 6.5 million**, reflecting a scalable and proportionate deployment model.

e. Feasibility (+)

From a technical perspective, the deployment of the EU Digital Police Cloud is feasible, supported by robust advancements in cloud computing and data analytics technologies, and notably via a more robust market offering including under sovereignty aspects. The initiative benefits from a solid foundation of Europol's existing expertise in secure data processing and with IT resilience across JHA agencies, ensuring that the infrastructure meets the high demands of law enforcement applications.

From a political perspective, there is broad support for the proposal given its alignment with EU objectives relating to enhanced security, digital sovereignty, and collaborative law enforcement. While recognising the strategic importance of unified crime prevention capabilities across the Union, sovereignty, security and data ownership, will be essential criteria to be met to comfort MS readiness to cooperate in implementing shared infrastructure.

The Europol Support Offices are operationally feasible, as they build on existing structures (Europol National Units), leverage Europol's current practice of temporarily deploying staff to support investigations and can make use of the Agency's secure IT and forensic environments, which could be extended to support this model.

From a **legal perspective**, the measure would require a targeted legislative amendment introducing an explicit legal basis for the establishment of Europol support offices in Member States limiting to support, coordination and technical functions, for the purpose of facilitating and strengthening operational support.

From a **political perspective**, the establishment of support offices would be demand-driven and voluntary, based on an invitation or agreement with the host Member State. The exact size, number, location and duration of Europol support offices would remain flexible and subject to periodic review.

f. Impact on digitalisation (++)

Digitalisation brought about by the EU Digital Police Cloud facilitates superior analytical capabilities, enabling Europol to process increasingly complex and voluminous datasets with greater precision and speed. This transformation accelerates the timeliness and accuracy of operative activity, promoting proactive threat identification and intervention strategies.

The cloud's sophisticated data handling and integration capacities afford Europol and national law enforcement authorities the opportunity to harness machine learning and AI-enhanced insights, fostering innovative approaches in combating organised crime and terrorism. Through these technological advancements, Europol and national authorities are better equipped to adapt to evolving criminal modalities, ensuring resilient and forward-thinking security strategies.

Europol Support Offices would enhance the digitalisation of law-enforcement cooperation by enabling earlier and more effective use of Europol's platforms and tools, improving data quality and interoperability, facilitating faster digital information exchange, and supporting the deployment of mobile digital tools during operations. By embedding expertise at national level, the option bridges the gap between technical capabilities and operational use, complementing EU efforts on interoperability, secure information exchange, and digital transformation.

ANNEX 11: COMPETITIVENESS CHECK

1. Overview of impacts on competitiveness

Dimensions of Competitiveness	**Impact of the initiative (++ / + / 0 / - / -- / n.a.)**	**References to sub-sections of the main report or annexes**
Cost and price competitiveness	n.a.	Main report – sections on economic impacts / stakeholders affected (initiative targets public authorities)
International competitiveness	n.a.	Main report – sections on economic impacts / stakeholders affected
Capacity to innovate	n.a.	Main report – sections on economic impacts / stakeholders affected
SME competitiveness	n.a.	Main report – "Application of the 'one in, one out' approach" (no admin costs for private sector)

2. SYNTHETIC ASSESSMENT

Overall, this initiative aims to address challenges related to the efficiency of Europol and to strengthen the implementation and further development of EU law enforcement cooperation. The measures under consideration primarily concern the organisation, planning, governance, operational cooperation and internal capacities of public authorities (Europol and Member States' competent law enforcement authorities). They do not introduce regulatory obligations for economic operators, do not set product requirements, and do not alter market access conditions or the rules governing competition in the internal market.

Accordingly, no direct impacts on competitiveness are expected across the four dimensions (cost/price competitiveness, international competitiveness, capacity to innovate and SME competitiveness). For the purposes of the competitiveness check, the initiative is therefore assessed as not applicable.

While the implementation of some measures may entail public procurement by Europol or Member States (e.g. for technical equipment and related services, including IT components, data processing tools, integration, maintenance, training or other support services), this reflects how public authorities may operationalise the measures, rather than an impact stemming from new requirements on undertakings. Such procurement would be conducted under the applicable EU and national public procurement rules and would not, in itself, constitute a competitiveness effect attributable to the initiative (no new compliance burden or market constraint is created for operators, including SMEs).

Stakeholder input from economic operators received during the Call for Evidence does not alter this conclusion, as the initiative remains focused on public-sector operational capacity, information exchange and governance in the area of law enforcement cooperation, rather than on regulating private-sector activity.