EUROPEAN
COMMISSION

Brussels, 24.6.2026
SWD(2026) 581 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE 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) 580 final} - {SWD(2026) 582 final}

A. Need for action

What is the problem and why is it a problem at EU level?

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

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

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[1], 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 frontiers[2]. As its mandate and tools have evolved, Europol has become a central pillar of a more integrated and operational European security architecture.

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[3] and in the evaluation of Europol[4], 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.

Two main problems have been identified:

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

[1] 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.
[2] 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.
[3] COM(2025) 752 final.
[4] See Annex 7.

- Europol's operational support remains limited and fragmented.

Objectives: What should be achieved?

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.

Specifically, the initiative aims to:

- Reinforce Europol's role as an information hub for law enforcement.
- Strengthening Europol's capacity to support law enforcement operational action

What is the added value of action at EU level (subsidiarity)?

Europol plays a unique and indispensable role in supporting Member States in preventing and combating serious 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. 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.

B. Solutions

What are the various options to achieve the objectives? Is there a preferred option?

Two main policy options were considered.

The **first option** focuses on targeted improvements to the existing operational model, which would strengthen Europol's support to Member State investigations. This would include improving data availability, timeliness and operational use. Key measures include targeted data-sharing obligations in priority crime areas, mandatory deployment of automated data-loader tools, and major upgrades to Europol's ICT systems to enhance automation, interoperability and analytical capabilities. Europol would also provide technical support, common standards and training to ensure operational benefits for Member States. Under this approach, measures would also improve the implementation of Data Subject Categorisation (DSC) without changing the legal framework, notably through advanced analytical tools and updated procedures. This first option would also enhance cooperation with Union bodies and agencies. In particular, it would enhance Europol's analytical support to EPPO investigations through dedicated expertise and closer coordination, improve the Europol-Eurojust operational continuum through more automated information-sharing and specialised support for accessing electronic evidence, and enable structured exchanges with AMLA via a hit/no-hit system to better identify links between financial intelligence and serious organised crime. At the same time, the second option would integrate Europol's analytical capabilities directly into national

investigations by connecting national case management systems with Europol's databases and tools.

The **second approach** envisaged a more structural evolution of Europol's operational model. It aimed to move beyond a framework centred primarily on bilateral information transmission towards the development of shared Union-level communication infrastructures, notably the EU Police Shared Data Space. This approach would also simplify Data Subject Categorisation (DSC) by aligning the Europol Regulation with the EUDPR and the Law Enforcement Directive. Instead of requiring categorisation before all data processing, DSC would apply where relevant and possible due to the nature of the data. This would improve Europol's ability to process large and complex datasets, while maintaining strong data protection oversight by the EDPS. This approach also provides for a more integrated form of operational support embedded directly within national investigative environments, including through the establishment of Europol Support Offices in Member States. In addition, this option also includes reinforced cooperation with the European Public Prosecutor's Office from a request-based model into a systematic and structured partnership.

On this basis, the **preferred option** combines elements of both approaches. It builds on the incremental improvements identified under the first approach, in particular as regards strengthening data availability, upgrading systems and embedding Europol tools into national investigations. At the same time, it goes beyond the existing model where necessary to address structural limitations, notably by enabling authorised access to national data, reinforcing Europol's operational presence in Member States, and strengthening its cooperation with the European Public Prosecutor's Office. These measures are designed to be mutually reinforcing. In particular, the incremental improvements under the first approach create the conditions for the more advanced measures to operate effectively, ensuring that enhanced data availability, systems and workflows support the use of new operational capabilities at Union level.

C. Impact of the preferred option

What are the benefits of the preferred option (if any, otherwise the main ones)?

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

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

estimated savings of approximately EUR 42 million compared to separate implementation approaches

The interferences with the rights to privacy and protection of personal data resulting from the preferred option remain necessary and proportionate having regard to the objective of ensuring effective prevention and combating of serious and organised crime and terrorism in an increasingly digital and cross-border operational environment. The impact assessment concluded that the current framework no longer adequately reflects the operational realities of modern criminal intelligence and creates structural limitations affecting Europol's ability to support Member States effectively. At the same time, the proposal substantially strengthens and restructures the safeguards framework applicable to Europol's processing activities. In particular, it introduces a more detailed legal and technical framework governing Europol's data environments, processing regimes, access conditions, separation of processing environments, logging and traceability requirements, storage periods, and supervisory and oversight mechanism.