EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Opinion 18/2026

on the Proposal for Regulation on Europol repealing Regulation (EU) 2016/794

edps.europa.eu

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'… for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

Wojciech Rafał Wiewiórowski was appointed as Supervisor on 5 December 2019 for a term of five years. The selection procedure for a new EDPS mandate for a term of five years is still ongoing.

Under Article 42(1) of Regulation 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data'.

This Opinion relates to the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation (Europol), amending Regulation (EU) 2018/1726 and Regulation (EU) 2024/982, and repealing Regulation (EU) 2016/794[1]*.*

This Opinion does not preclude any future additional comments or recommendations by the EDPS, in particular if further issues are identified or new information becomes available. Furthermore, this Opinion is without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Regulation (EU) 2018/1725.

This Opinion is limited to the provisions of the Proposal that are relevant from a data protection perspective.

[1] COM(2026) 580 final.

Executive Summary

On 24 June 2026, the European Commission issued the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation (Europol), amending Regulation (EU) 2018/1726 and Regulation (EU) 2024/982, and repealing Regulation (EU) 2016/794.

The objective of the Proposal is to strengthen the legal framework of Europol, in line with the evolution of cross-border criminal threats and the operational needs of Member States. It aims in particular to strengthen Europol's role as EU information hub, operational hub and technology and innovation hub.

While the EDPS supports the overall objective of the Proposal of reinforcing Europol's role in supporting Member States' law enforcement authorities and their mutual cooperation, he stresses that the choices that will be made by the Union legislator will have a lasting impact on how the EU reconciles the need to ensure security for its citizens with the protection of fundamental rights. It is therefore critical that the new Regulation sets out a clear and comprehensive legal framework, consistent with the role entrusted to Europol by EU primary law, which provides both minimum safeguards and appropriate mechanisms for effective oversight and enforcement of EU data protection laws.

The EDPS is particularly concerned by the serious risks for the right to the protection of personal data arising from the envisaged possibilities for Europol to process personal data pertaining to individuals with no established links to criminal investigations or proceedings, i.e. processing of data of persons not categorised depending on the type of link with the criminal investigation. The Proposal would enable Europol to retain data of vast number of individuals with no established connection to a criminal activity for an extensive and unspecified period of time. The EDPS considers that the Proposal in its current form fails to provide sufficient and effective safeguards in such situations.

To this end, the EDPS makes a number of specific recommendations aimed at ensuring a high level of legal clarity and legal certainty of the Proposal as well as foreseeability, transparency and accountability regarding the new processing powers entrusted to Europol.

The EDPS also comments upon and provides specific advice, among others, on the proposed rules for access and query of Europol systems; the processing of personal data obtained directly from private parties; the supervision of data processing activities carried out by Europol staff in Member States and his cooperation with the national supervisory authorities; security of Europol services and tools; and others.

Contents

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ('EUDPR')[2], and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1. On 24 June 2026, the European Commission issued a 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[3] ('the Proposal').

2. The objective of the Proposal is to strengthen the legal framework of Europol, in line with the evolution of cross-border criminal threats and the operational needs of Member States. It aims in particular to strengthen Europol's role as:

   - EU information hub providing Member States law enforcement authorities with a more complete and integrated criminal intelligence picture at EU level;

   - operational hub supporting Member States more effectively and at an earlier stage in cross-border investigations and operational activities; and

   - technology and innovation hub supporting Member States with advanced capabilities, expertise and operational tools[4].

3. The Proposal on Europol is part of a bigger Justice and Home Affairs (JHA) legislative package, which also includes proposals to strengthen the mandate of the EU Agency for Criminal Justice Cooperation (Eurojust), a targeted revision of the rules on processing of operational personal data in the EUDPR, and a recast of the Directive on European Investigation Order. The EDPS is issuing separate Opinions on each of these proposals.

4. The present Opinion of the EDPS is issued in response to a consultation by the European Commission of 25 June 2026, pursuant to Article 42(1) of EUDPR. The EDPS welcomes the reference to this consultation in Recital 132 of the Proposal. The EDPS also positively notes that he was previously informally consulted pursuant to recital 60 of EUDPR.

[2] OJ L 295, 21.11.2018, p. 39.
[3] COM(2026) 580 final.
[4] See COM(2026) 580 final, p. 4.

2. General remarks

5. The EDPS supports the overall objective of the Proposal, which aims at reinforcing Europol's role in supporting and strengthening Member States' law enforcement authorities and their mutual cooperation. The EDPS stresses that the choices that will be made by the Union legislator will have a lasting impact on how the EU reconciles the need to ensure security for its citizens with the protection of fundamental rights. It is therefore critical that the new Regulation sets out a clear and comprehensive legal framework, consistent with the role entrusted to Europol by EU primary law, which provides both minimum safeguards and appropriate mechanisms for effective oversight and enforcement of EU data protection laws.

6. The substantial expansion of Europol's tasks and data-processing capabilities under the Proposal would entail not only a quantitative increase in the volume of personal data processed but also involve new, diverse, and materially more complex processing operations concerning additional categories of personal data and of data subjects, including individuals with no verified links to criminal investigations or proceedings. The Proposal foresees new and increasingly automated information flows with a wide range of different stakeholders, including, most notably, intensified exchanges of large amounts of personal data with national authorities and, in certain cases, third countries and private parties. Against this background, the EDPS underlines the need for adequate oversight framework to verify compliance with the applicable data protection safeguards, as well as a corresponding allocation of human and financial resources for the supervision of Europol, thus ensuring a credible supervisory capacity of the EDPS for the reformed Agency.

7. The EDPS recognises that the Union and its Member States are facing increasingly complex, technologically sophisticated cross-border crimes and internal security threats, which require further development and enhancement of Europe's security architecture. At the same time, it is crucial for the new Europol Regulation to meet high level of legal clarity and legal certainty to ensure foreseeability, transparency and accountability regarding the new processing powers entrusted to Europol. Without clear data protection rules regulating the new processing powers of Europol, the possibility for the EDPS to ensure effective supervision will also be affected, to the detriment of fundamental rights of concerned data subjects.

8. The EDPS is particularly concerned by the envisaged new possibilities for Europol to process personal data pertaining to individuals with no established links to criminal investigations for extended periods of time and for a broad range of purposes. In this regard, he has serious doubts that the current Proposal satisfies the requirements of foreseeability, necessity and proportionality[5].

9. This Opinion aims to provide constructive and objective advice with a view of ensuring that the Proposal provides for the appropriate level of data protection, while delivering on its main policy objectives.

[5] See also EDPS toolkit: Assessing the necessity of measures that limit the fundamental right to the protection of personal data issued on 11.4.2017, EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data issued on 19.12.2019, as well as EDPS Guidance for co-legislators on key elements of legislative proposals, issued on 07.052025.

3. Data subject categorisation

10. The EDPS recalls that the 2022 reform of the Europol Regulation[6], in particular the new Articles 18(6a) and 18a, introduced the possibility for Europol to process personal data that fall outside the exhaustive list of categories of personal data and of data subjects whose data may be collected and processed by the Agency, laid down in Annex II. B. of Europol Regulation,[7] in exceptional cases and for a limited amount of time. When the EDPS was consulted on the Proposal at the time, he recommended introduction of efficient safeguards in Article 18a, in order to ensure that this derogation is applied on an exceptional basis and thus prevent the risk of the exception becoming the rule[8].

11. The Proposal would take it one step further, however, by including such processing into the list of purposes for which Europol can process personal data, converting an exceptional situation into a regular activity. As a result, Europol would no longer be bound by the rules currently applying to the processing of personal data of data subjects falling outside the categories listed under Annex II of Europol Regulation.

12. According to Article 32(7) of the Proposal, Europol would be allowed to process personal data of individuals outside of the categories of data subjects listed in Annex II, i.e. with no link to a criminal activity, where such processing is deemed 'relevant and necessary' for the purposes defined in paragraph 2 of the same Article.

13. The EDPS recalls that pursuant to Article 18(6a) of the current Europol Regulation, Europol has been given the legal possibility to process data pertaining to individuals with no established link to a criminal activity, but only to the extent that such processing is required to carry out a pre-analysis of personal data received in the context of preventing and combating crimes that fall within its objectives for the sole purpose of establishing whether they relate to one of the categories of data subjects listed in Annex II. The EDPS further notes that Article 18a of the current Europol Regulation, which allows the Agency to process personal data outside of the categories of data subjects listed in Annex II, limits the purpose of such processing only to 'ongoing specific criminal investigation within the scope of Europol's objectives', while the Proposal refers to all the purposes laid down in Article 32(2). The EDPS considers that not all of these purposes listed in Article 32(2) could justify such a serious interference with the right to the protection of personal data.

14. The EDPS considers that the new envisaged possibilities for Europol to process personal data pertaining to individuals with no established links to criminal investigations or proceedings (i.e. processing of data which have not undergone the so-called data subject categorisation process) constitutes a very serious interference with the right to the

[6] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, (OJ L 135, 24.5.2016, p. 53, as amended by Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, OJ L 169, 27.6.2022, p. 1.

[7] Annex II to the ER (under B(1)(a)-(f)) specifies the categories of persons whose personal data are processed by Europol for the purpose of analysis of a strategic or thematic nature, for operational analysis or for facilitating the exchange of information between Member States, Europol, other EU bodies, third countries and international organisations. The Regulation differentiates between six categories: (a) suspects or convicted persons; (b) persons who are likely going to commit an offence; (c) witnesses; (d) victims; (e) contacts and associates; (f) informers.

[8] EDPS Opinion 4/2021 on the Proposal for Amendment of the Europol Regulation, https://www.edps.europa.eu/system/files/2021-03/21-03-08_opinion_europol_reform_en.pdf, paragraph 29.

protection of personal data. The Court has consistently held that legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued[9]. Coupled with the expansion of Europol's mandate where the Agency will be called to process larger volume of unstructured datasets, the Proposal would lead to the multiplication of potential situations where data processing could not be justified as necessary and proportionate, while at the same time not being subject to effective data protection safeguards or supervision.

15. The EDPS further notes that the new possibilities to process data included in large and unstructured datasets would also apply to data received from private parties or collected from the internet (OSINT). The EDPS underlines that, in such cases, Europol's processing of personal data that have not undergone data subject categorisation process would be enabled regardless of whether it complies with the laws of the Member States applicable to the use of such data, including on the oversight of the lawfulness of the processing by the competent national judicial authorities.

16. Article 32(6) of the Proposal provides that Europol must distinguish between categories of data subjects only '*where applicable and as far as possible*'. The Explanatory Memorandum to the Proposal[10] explains that the provision is essentially an alignment with the rules on data subject categorisation under Regulation (EU) 2018/1725 (Article 73 EUDPR[11]). However, the EDPS would like to point out that Article 73 EUDPR does not provide a general legal basis for the processing of personal data of individuals that have no link to a criminal activity. The EDPS also recalls that in line with Recital 11 EUDPR, the new Europol Regulation constitutes *lex specialis* to the EUDPR. As such, it should complement the general EUDPR rules by laying down the specific conditions and safeguards that would ensure that the processing of data without data subject categorisation by the Agency remains limited to what is necessary and protects individuals against the risk of abuse. Currently the Proposal does not lay down such conditions and safeguards.

17. The EDPS considers an essential requirement for the new Regulation to ensure an adequate level of legal clarity and foreseeability of personal data processing by Europol. The Proposal in its current form, in light of the expansion of the possibility to process vast amounts of personal data of persons with unverified links with the objective pursued, does not fulfil these important requirements.

18. The Proposal would also have a direct impact on the exercise of data subjects' access requests, as Europol might not be able to identify individuals whose data are being processed in large unstructured datasets until they are analysed and categorised.

19. While the EDPS understands that these new provisions are meant to take stock of the reality of modern data-driven law enforcement, the Proposal does not address the serious risks for individuals' fundamental rights and freedoms. In its current form, the Proposal would enable Europol to retain data of vast number of individuals with no established connection to a criminal activity for an extensive and unspecified period of time.

---

[9] See in particular the judgment in joined case C-511/18, 512/18 and 520/18, La Quadrature du Net, para 133.

[10] See COM(2026) 580 final, Explanatory Memorandum, p. 14.

[11] Article 73 '***Distinction between different categories of data subjects.*** *The controller shall, where applicable and as far as possible, make a clear distinction between the operational personal data of different categories of data subjects, such as the categories listed in the legal acts establishing Union bodies, offices and agencies.*

20. The EDPS considers that the proposed rules related to the processing of personal data that have not undergone the data subject categorisation process do not meet the required level of legal clarity. The effect of such rules on the fundamental rights of data subject is not clearly foreseeable, since the Proposal does not provide for clear and precise definition of the scope and application of the measures in question (i.e. it does not clarify when the processing would effectively be '*necessary for Europol to fulfil its tasks*'). Moreover, the Proposal does not impose minimum safeguards as it provides only for a for a notification of Europol's data protection officer (DPO) without specifying any specific tasks of the DPO in this case[12], and for functional separation of different categories of data included in large and unstructured datasets only '*as far as possible*'[13] .

21. The EDPS has therefore serious doubts about the necessity and proportionality of the interference, since the Proposal does not set out clear limitations for this processing operation, either with regard to the data to be processed – categories of personal data have been removed from Annex II – or to the time limits of this processing – regular data retention regime applies.

22. Moreover, the EDPS is concerned that if the Proposal fails to provide sufficient and effective safeguards in situations where Europol processes personal data of individuals with no established link to a criminal activity, it might be deemed not compliant with the requirements of Article 52(1) of the Charter[14].

23. In this regard, the EDPS recommends that:

- the purposes in Article 32(2) of the Proposal that could justify processing of personal data of individuals outside of the categories of data subjects listed in Annex II should be strictly limited and, in principle, limited to ongoing specific criminal investigation within the scope of Europol's objectives;

- the Proposal should lay down clear maximum time limits on processing of uncategorised personal data, thus preventing situations where personal data of individuals with no link to any criminal activity stay in police databases for an extensive and undefined period of time;

- the criteria, based on which Europol would decide whether the processing of personal data of individuals outside of the categories of data subjects listed in Annex II, is 'relevant and necessary', should be defined either in the Regulation itself, or in a Management Board Decision after consultation with the EDPS. Such an approach would enhance legal certainty, minimise legal risks for Europol[15], and facilitate effective supervision by the EDPS[16]. Without clarification at legislative level (preferably directly

[12] See Article 32(8) of the Proposal.
[13] See Article 32(9) of the Proposal.
[14] The CJEU has made clear that EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must "lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary" – see e.g. Case C-623/17, para. 68 and the case law cited therein.
[15] See also the recent case law of the Court of Justice requiring law enforcement authorities to document the reasoning underpinning even routine operational measures, such as the fingerprinting (refer for example to Comdribus, C-371/24).
[16] If these criteria are not defined at the legislative level or through an appropriate empowerment, they will inevitably have to be developed by the EDPS in the exercise of its supervisory tasks. This would risk placing the EDPS in a position where it effectively shapes operational criteria.

in the text of the new Regulation), or, alternatively, through dedicated implementing rules), the meaning and content of the criteria related to relevance and necessity will have to be developed by the EDPS in the exercise of its supervisory tasks.

4. Access and query of Europol systems

24. The EDPS notes that the Proposal includes several provisions[17] enabling access to Europol systems by a wide range of different authorities. Relevant provisions in this regard relate, for instance, to the Europol cross-checking service (Article 36 of the Proposal); the Europol analytical environment (Article 40 of the Proposal); the Police Shared Data Space (Article 42 of Proposal), and the establishment of a new automated hit/no-hit system allowing for indirect access by other Union bodies, offices and agencies, where such access is provided for in Union law, to information held by Europol (Article 80 of the Proposal).

25. Chapter VIII 'Data protection' of the Proposal, which sets out the data protection rules applicable to Europol's data processing activities, is deemed to apply to the processing operations of the above-mentioned services and tools. At the same time, Chapter VIII does not lay down any specific requirements regulating the processing of different categories of personal data, including special categories of data and/or data of specific categories of data subjects such as victims, in case of access and use, by different actors, of the abovementioned Europol's services and data processing tools. The relevant provisions of the proposed Regulation refer to implementing acts, but only to indicate that such instruments will provide the technical specifications and data security requirements to implement the related Europol's services and data processing tools.

26. The EDPS recommends that the Proposal should specify the specific requirements applying to the processing of different categories of personal data during the access and use of Europol services and data processing tools referred to under Section II of Chapter III by other Union or Member States bodies, as well as through the new indirect information exchange on the basis of a hit/no-hit system, as referred to under Article 80 of the Proposal. The respective roles and data protection responsibilities should also be specified[18] If not specified in the main legal instrument, i.e. the Europol Regulation itself, these aspects should at least be defined in respective implementing acts envisaged in the Proposal.

27. In the same vein, the EDPS recommends that the Proposal should define, even if only in a general manner, the categories of personal data that would be included in the index(es) of the hit/no hit system laid down in Article 80 of the Proposal, which could then be further specified in the implementing act provided for in Article 80(9)) of the Proposal.

28. Furthermore, in the interest of transparency, the EDPS recommends requiring Europol to make publicly available and keep up to date an overview of the which Union and Member States authorities would have direct access to Europol systems.

29. In addition, the EDPS notes that Articles 39(2)(c) and 41(2)(c) of the Proposal introduce the possibility to query Europol systems, namely the Europol cross-checking service and the Europol Analytical Environment, not only with alphanumeric and biometric, but also with

[17] See in particular Section 2 of Chapter III of the Proposal.
[18] See further also section 8 of the Opinion ('Responsibility in data protection matters').

'multimedia data'. In view of legal certainty, the EDPS recommends clarifying in the Proposal the meaning and the content of 'multimedia data'.

5. Systematic use of biometric data to query the Europol Analytical Environment

30. The EDPS notes that pursuant to Article 41(2) of the Proposal, 'Europol shall query the Europol Analytical Environment to carry out its tasks, including biometric data for the purpose of uniquely identifying a natural person'[19]. This provision, read in conjunction with Recital 106 of the Proposal, would enable the systematic use of sensitive categories of data, i.e. biometric data processed for the purpose of uniquely identifying a natural person, to query Europol's Analytical Environment.

31. Article 100(2) of the Proposal indicates that the processing of biometric data for the purposes uniquely identifying a natural person shall only be allowed where strictly necessary and proportionate for the purposes set out therein. Recital 106 expressly clarifies that processing of biometric data for the purpose of uniquely identifying a natural person by Europol through the access to and query of the Europol Analytical Environment should be considered as '*strictly necessary*' for preventing or combating crimes falling within the scope of Europol's competence. As currently drafted, the Proposal could be read as implying that the processing of biometric data mentioned in 41(2) and recital 106 of the Proposal would be strictly necessary 'by default', without the need for a case-by-case assessment.

32. The EDPS recalls that in Case C-371/24 Comdribus, the CJEU established that Directive 2016/680[20] precludes the systematic collection of biometric data of any person reasonably suspected on one or more grounds of having committed or attempted to commit a criminal offence, unless the national law defines '*the specific and concrete purposes pursued by that collection in an appropriate and sufficiently precise manner and the competent authority is required to assess, in each case, whether that collection is strictly necessary for achieving those purposes*'[21]. The Court also found that it must be assessed, in any event, whether that collection is '*strictly necessary in the light of all the relevant factors*'. The EDPS considers that the same requirements apply, by analogy, to Europol's processing of biometric data for the purpose of querying the Europol Analytical Environment.

33. The EDPS considers that the Proposal should provide for a mandatory case-by-case assessment of both the strict necessity and proportionality of the query of the Europol Analytical Environment using biometric data processed for the purpose of uniquely identifying a natural person. To this end, a specific provision should be introduced and Recital 106 of the Proposal should be amended accordingly.

[19] An identical provision with the same wording is included in Article 41(5) of the Proposal. The EDPS understands this repetition to be a clerical error.
[20] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119, p. 89.
[21] See Judgment of the CJEU in Case C-371/24 Comdribus, ECLI:EU:C:2026:219, para. 91.

6. Processing of personal data obtained directly from private parties

34. The EDPS notes that, pursuant to Article 96 of the Proposal, Europol would be allowed to process personal data originating directly from private parties, 'insofar as it necessary for the performance of its tasks'. As no limitation is provided, it may extend to any type of personal data (including personal data originally collected for commercial purposes), regardless of whether such processing has been requested or authorised by a competent national authority.

35. As result, Article 96 of the Proposal may enable Europol to process potentially large amounts of personal data received directly from private parties, including data pertaining to individuals not linked to a criminal investigation or offence, and which may not be subject to judicial supervision of the compliance of such processing with the applicable laws of the concerned Member States. It could even be interpreted as enabling processing in cases where no Member State is concerned.

36. The EDPS recommends that the proposed Regulation should maintain the logic of Article 26(2) of the current Europol Regulation, according to which Europol may as a rule process data received from private parties first and foremost in order to identify the Member State concerned. Derogations to such rule, i.e. processing for purposes that go beyond the purpose of identifying the Member State(s) having jurisdiction in the case, should only be allowed in specific circumstances, clearly circumscribed in the Proposal.

7. Description of Europol's tasks

37. The EDPS notes that, in contrast to Article 4 of the current Europol Regulation, which defines Europol's tasks through an extensive and detailed list of activities, Article 6 of the Proposal structures Europol's competences around its principal functions and responsibilities, namely information processing and criminal intelligence, operational support, strategic and operational analysis, cooperation with Union bodies, offices and agencies, third countries and international organisations, and research and innovation activities. The detailed rules governing the exercise of those functions, including the applicable procedures, powers, conditions and safeguards, are set out in the relevant substantive chapters[22].

38. While understanding the aim of the Proposal to provide for certain level of flexibility for Europol, the EDPS observes that the level of precision as to the exact nature, scope and limits of the tasks of the Agency, including regarding the related data processing powers, differ, sometimes significantly, between the different mandated tasks. For instance, the Proposal does not seem to provide for any specific safeguards in case of processing of personal data for strategic analyses purposes, unlike operational analyses and research and innovation purposes, for which a number of additional conditions are laid down.

[22] See (2026) 580 final, Explanatory Memorandum, p. 15.

39. In the interest of legal certainty and foreseeability, the EDPS stresses the importance of consistently laying down in the substantive chapters of the Proposal dedicated to the specific tasks entrusted to Europol clear rules setting out the procedures, conditions and the specific safeguards applicable to the exercise of related personal data processing activities accompanied by an adequate statement of reasons in the respective recitals

40. In the same vein, the EDPS recommends that the Proposal should cross-reference each of the tasks of the Agency laid down in Article 6 with the corresponding specific provisions / chapters governing the respective activity.

8. Responsibility in data protection matters

41. The EDPS recalls that Article 38 of the current Europol Regulation allocates responsibilities in data protection between Europol and Member States. It regulates the current setting where Member States send data to Europol for purpose of criminal intelligence activities and where Europol offers a secure communication channel for exchanging operational data (SIENA).

42. The Proposal introduces new forms of processing of personal data by which Europol and Member States jointly process data for purposes of operational analysis, such as Joint Operational Analysis Cases, or where Europol provides Member States with new tools, such as a secure cloud. In this regard, the EDPS notes that Article 107 'Responsibility in data protection matters' does not clearly allocate responsibilities for such new forms of processing under data protection law.

43. In particular, the Proposal does not expressly and consistently clarify the role of Europol under data protection law (i.e. as controller, joint controller) in relation to the different processing activities it carries out, often in close cooperation with multiple actors[23]. Similarly, Recital 128 of the Proposal states that when Europol conducts searches using biometric data originating from Member States, it should act 'solely as a technical and forensic service provider on behalf of the authorising Member State' but stops short of defining its role as processor. Conversely, Article 96(9) of the Proposal explicitly clarifies Europol's role as a processor in cases where Member States authorities use Europol's mechanism for the exchange of personal data with private parties, for crimes not falling under Europol's competence.

44. The EDPS considers that a clear definition, at the level of legislation, of respective roles and data protection responsibilities of the actors involved in personal data processing, reflecting operational reality, is essential to legal certainty, and critical for enabling effective oversight by competent data protection authorities at EU and national level. The attribution of data protection roles also directly effects the effective exercise of data subjects' rights. [24]

45. The EDPS therefore strongly recommends defining the roles and responsibilities of Europol and Member States in a comprehensive manner. In addition, the EDPS recalls that any

[23] See in particular Operational task forces (Article 20); Europol deployments for operational, technical, analytical, and forensic support to Member States and, where applicable, non-EU countries (Article 22); the Police Shared Data Space (Article 42); Joint Operational Analysis Cases (JOACs) (Articles 43 to 45),
[24] See EDPS Guidance for co-legislators on key elements of legislative proposals, issued on 7 May 2025, para 25-26.

relationship between (joint) controllers and processors must be governed by appropriate legal arrangements[25]. Alternatively, if these roles and responsibilities are not to defined exhaustively in the Proposal as such, an empowering clause should be provided to further define the roles and responsibilities through implementing acts.

9. Supervision of data processing activities carried out by Europol staff in Member States

46. The EDPS notes that pursuant to Article 112(1) of the Proposal, the national supervisory authorities referred to in Article 41 of Directive (EU) 2016/680 would have the power to access data submitted by their Member State to Europol. The Proposal would also grant the above-mentioned national supervisory authorities with the power to access logs, as currently referred to in Article 88 EUDPR. The access to such data and logs by national supervisory authorities would be granted as far as it takes place in accordance with the relevant national procedures, and in so far as such activities are relevant to the protection of personal data (Article 112(2) of the Proposal). In practice, national supervisory authorities' access to the above-mentioned data and logs would take place at the Europol national unit and at the liaison officers' premises.

47. The EDPS welcomes this element of the Proposal, which he considers as a step toward the creation of enhanced cooperation mechanisms for coordinated supervision between the EDPS and national supervisory authorities.

48. At the same time, the EDPS is concerned that the Proposal does not provide for a similar power for the EDPS to access data and logs related to processing operations concerning data submitted by Europol to the Member States. Introducing this specific power for the EDPS appears essential for ensuring continuous supervision of the processing activities carried out by Europol staff regardless of the environment in which they are performed.

49. The EDPS therefore recommends including in the Proposal a provision expressly granting the EDPS the power to supervise the data processing activities carried out by Europol staff embedded within national investigative environments, in particular though the establishment of Europol Support Offices in the Member States (Article 26).

50. The Proposal should also clarify that any person should have the right to request the EDPS to verify the legality of any transmission or transfer or communication by Europol to the Member States of data concerning him or her. That right should be exercised in accordance with the Article 84 EUDPR. The inclusion of such provision would also be consistent with Article 112(4) of the Proposal laying down a similar right of data subjects vis-à-vis national supervisory authorities.

[25] See also EDPS Guidance for co-legislators on key elements of legislative proposals, issued on 7 May 2025, para 28-35.

10. Consultation with the national supervisory authorities by the EDPS

51. Article 113(4) of the Proposal obliges the EDPS to consult national supervisory authorities on cases relating to data originating from one or more Member States, and to await their opinion before deciding on further action. On substance, it reproduces the provision of Article 44 (4) of the current Europol Regulation.

52. Based on his supervisory experience, the EDPS notes that the envisaged deadline for such consultation - between one and three months – is often insufficient for national supervisory authorities to complete their checks and deliver a substantiated opinion, particularly for the more complex cases requiring onsite checks. However, the provision of Article 113(4) of the Proposal, similarly to the existing Article 44(4) Europol Regulation, does not contain any mechanism to resolve situations where a national supervisory authority does not respond within the deadline, leaving the EDPS without a clear pathway forward, thus creating potential deadlocks.

53. The EDPS therefore recommends extending the maximum deadline from three to six months, giving national supervisory authorities a more realistic timeframe to complete their checks, while the EDPS retains discretion to set a shorter deadline (not less than one month) where appropriate. In addition, the EDPS recommends introducing a presumption of agreement of the national supervisory authority with the position of the supervised law enforcement authority where the former does not deliver its opinion within the deadline set by the EDPS.

11. Time limits for prior consultations

54. The EDPS notes that Article 108(1) of the Proposal, concerning prior consultation of Europol with the EDPS, provides for different time limits for the delivery of a written advice by the EDPS compared with the horizontal provision on prior consultations - Article 90(4) EUDPR - even if the Proposal specifically refers to the latter provision. In particular, Article 108(1) of the Proposal lays down a deadline of 8 weeks without a possibility of extension, while Article 90(4) EUDPR provides for a period of up to six weeks, which may be extended by a month, taking into account the complexity of the intended processing.

55. Prior consultations typically concern complex and novel processing operations that require a thorough assessment of extensive technical, operational and governance documentation, as well as a detailed understanding of the safeguards and procedures envisaged by the controller. Such processing activities are often the product of many months, and in some cases years, of development and refinement by Europol. It is therefore essential that the supervisory authority is afforded sufficient time to examine the relevant materials and engage meaningfully with the issues raised, including to request complementary information not previously provided, in order to provide informed and effective advice.

56. Moreover, the EDPS recalls that one of the objectives of the Proposal is full alignment of the legal framework of Europol with the EU's data protection framework, in particular the

EUDPR[26]. The EDPS therefore recommends an actual alignment of the time limits for prior consultations in Article 108(1) of the Proposal with the timeline provided for in Article 90(4) EUDPR.

57. The EDPS also notes that the proposed reform of the 'urgency procedure' (Article 108(2)) (i) removes the requirement that the consultation is underway before the processing starts, (ii) replaces the full consultation dossier with a summary notification and an initial rather than complete risk assessment, and (iii) grants a four-week filing period unconnected to any demonstrated need. In this way the Proposal is decoupling the urgent processing from the consultation procedure itself and risks converting an *ex ante* procedure to an *ex post* one.

58. The EDPS therefore recommends targeted corrections in order to preserve the Proposal's operational gains while maintaining to the extent possible the nature of the prior consultation mechanism. In particular, the EDPS recommends:

    - introducing a requirement for submitting the complete prior consultation request 'without undue delay' and in any event within a shorter period than the one provided in the Proposal, and

    - obliging Europol to substantiate, in the initial notification, why the complete assessment could not be finalised before the start of the processing operation.

12. Notification of a personal data breach

59. The EDPS notes that Article 103 of the Proposal clarifies how Europol should act in case of a personal data breach, and in particular its obligations to notify the competent authorities of the Member State concerned of the data breach and the providers of the data. In this regard, the EDPS finds the wording of paragraph 1 of the provision not entirely clear as it could be interpreted that competent authorities of the Member States would be notified without undue delay and in all cases of personal data breaches concerning them, whereas the provider of the concerned data, in case it is not a competent authority of a Member State (e.g. third-countries, private parties), would be notified only if the personal data breach is likely to result in a risk to the rights and freedoms of the natural persons.

60. The EDPS supports the rule that the competent authorities of the Member State concerned of the breach should always be notified, without undue delay. This will ensure that they can take the elements of the personal data breach into account for their processing activities and further assess potential additional risks for the data subjects, in the context of their processing activities. This requirement, apart from being in line with article 92(5) of EUDPR, would also ensure timely notification of competent authorities in case Europol acts as their processor.

61. At the same time, as already explained above, Article 103(1) of the Proposal might be understood as introducing a higher threshold for notifying data providers other than the Member States competent authorities. The EDPS reminds that in some cases Europol may

[26] See COM(2026) 580 final, p. 7.

have only a limited view of the risks to data subjects, considering that the received data might form part of a bigger dataset and/or may be subject to other data breaches enabling to correlate data. Furthermore, the EDPS reminds that in cases where the provider of the data is a natural person (via the channels provided for by Article 97 of the Proposal), the data breach might create additional specific risks for him or her.

62. For the above reasons, the EDPS considers that all providers of personal data should be notified about breaches concerning data they have provided in all cases and without undue delay, in order to ensure adequate assessment of risks and informing affected data subjects where necessary.

13. Security of Europol services and tools

63. The EDPS positively notes that Section 2 of Chapter III of the Proposal offers a description of the main information systems, services and tools offered by Europol. The introduction of these descriptions in the legal framework of Europol will enhance transparency and will inform future decisions on interoperability with Europol information systems, when provided for in the Union legislation.

64. At the same time, the EDPS notes that the Commission may introduce changes and additions to these services and tools by way of implementing acts. In this context, the EDPS would like to underline the importance of maintaining and making available to the EDPS an up-to-date catalogue of all services and tools and the purposes for which they may be used.

65. The EDPS would also like to remind that the use of any tool or technology should be seen in conjunction with the activity and the purpose for which it is deployed. The same tool or technology could create different risks in different use cases. For that reason, the EDPS underlines the importance of carrying out a thorough data protection impact assessment before introducing new functionalities in existing services and tools and before re-using them for new purposes.

66. The EDPS notes that the Proposal contains only general references to the security of operational personal data across information systems. In this regard, the EDPS reminds that Europol should guarantee a full compliance with the horizontal provision on the security of processing of operational personal data - Article 91 EUDPR. The EDPS considers that the Agency should, in addition to complying with Article 91 EUDPR, be explicitly required to establish and maintain appropriate security governance documentation and procedures, including security and data protection risk assessments, security plans, business continuity plans and disaster recovery plans, covering all systems, infrastructures and interoperability components involved in the processing of operational data.

67. In the same spirit, the EDPS notes that Article 50 of the Proposal establishes the Europol cloud infrastructure as a secure and scalable platform of cloud computing services enabling Europol and competent authorities of the Member States to access Europol's tools, collaborative environments and other operational and analytical capabilities. Pursuant to Article 50(4) of the Proposal, 'Europol shall ensure that the procurement of cloud computing services complies with applicable Union law, including requirements on the EU cloud sovereignty framework, data security, data protection, cybersecurity and digital sovereignty'.

68. The EDPS has been formally consulted on the Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem ('Cloud and AI Development Act' or 'CADA'). In this context, he notes that pursuant to Article 30(3) of the Proposal for CADA, the cloud computing services procured by Union entities and public sectors bodies in the areas of national security, internal security, external border management, defence, justice or law enforcement, including the prevention, investigation, detection and prosecution of criminal offence must have a Union assurance level 2, 3 or 4 (level 1 being the least secure and level 4 the most secure). However, according to paragraph 4 of the same Article, in certain cases, the assurance level could be further lowered to level 1, e.g. for financial reasons.

69. The personal data collected for internal security, border management, justice, or law enforcement purposes are typically highly sensitive. In this context, a potential data breach, including access to the data by third countries or other unauthorised third parties might have a very serious consequences not only for the affected data subjects, but also for the competent Union or Member States authorities. The security of the cloud services is also critical for the Union agencies and large-scale IT systems in the field of justice and home affairs, which act as information hubs and/or databases at Union level and contain millions of records, including biometric data.

70. For these reasons, the EDPS stresses the crucial importance that the cloud computing services in the areas of internal security, border management, justice or law enforcement, procured by Union bodies, and in particular Europol as the central information hub for internal security of the Union, should meet the highest Union assurance levels (preferably level 4 but in any event not lower than level 3).

71. In addition, the EDPS notes that Article 54 of the Proposal introduces the obligation for Europol to develop, implement and maintain an EU DNA matching application for the purpose of enabling secure and reliable comparison of DNA profiles, in support of Member States investigation of criminal offences. Annex 9 to the Impact Assessment accompanying the Proposal[27] clarifies the future EU DNA matching application would address a structural technological dependency of the EU on a third country for a core component of its law enforcement infrastructure, namely the DNA profile comparison and exchange framework.

72. The EDPS strongly supports developing an EU-controlled DNA matching service, which would enhance the Union's technological sovereignty in a critical area of forensic cooperation, while ensuring full compliance with the Union legal framework on data protection.

14. Communication channels with ETIAS

73. According to Article 29(2) of the European Travel Information and Authorisation System (ETIAS) Regulation[28], in case of a hit with Europol data or the ETIAS watchlist, the ETIAS Central Unit should transmit the information of the applicant and the hits to Europol.

[27] SWD(2026) 580 final, pages 152-153.
[28] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, PE/21/2018/REV/1, OJ L 236, 19.9.2018, pp. 1–71.

Following this step and according to Article 29(4) of the ETIAS Regulation, Europol would provide a reasoned opinion on the application. Europol's opinion must be made available to the ETIAS National Unit of the Member State responsible which would record it in the application file. Pursuant to Article 29(7) of the ETIAS Regulation, the consultation request and the replies thereto must be transmitted through the software referred to in Article 6(2)(m) of ETIAS Regulation[29].

74. The EDPS notes that Article 31(5) of the Proposal refers to the Europol's obligation to provide a reasoned opinion via SIENA to the authority managing an application (VISA or ETIAS respectively), in cases of hits.

75. The proposed process departs from the workflow established under Article 29 of the ETIAS Regulation. Rather than transmitting a single, reasoned opinion directly to the competent ETIAS National Unit through the ETIAS information system, the supporting analysis would be communicated through a parallel procedure. Specifically, while the formal reasoned opinion would continue to be provided via the ETIAS software, an additional report containing the supporting operational information would be transmitted separately through SIENA to the Europol National Unit, which would then make that report available to the ETIAS National Unit of the Member State responsible, using means that are not further specified. This approach would effectively introduce an additional processing channel, an intermediary actor, and a separate processing operation for information that forms part of the same substantive assessment.

76. Introducing a parallel transmission mechanism outside the ETIAS workflow established by the ETIAS Regulation may undermine the transparency of the processing operations and the traceability and accountability of decision-making in the ETIAS framework. In addition, the proposed arrangement raises concerns regarding compliance with the principles of data minimisation. An additional transmission channel necessarily increases the number of processing operations, access points and entities involved in handling the personal data; the creation of duplicate records results in increased complexity in managing data subject rights, data accuracy, rectification, deletion, and retention obligations across multiple processing environments.

77. Should it be assessed that operational requirements necessitate the use of such a separate communication channel, the EDPS considers that appropriate technical and organisational measures should be put in place to ensure that the reasoned opinion and its supporting report remain available and linked throughout their lifecycle (e.g. ensuring that retention periods of both documents are aligned and that both documents carry a common unique case identifier recorded in all relevant systems, enabling the complete file to be reconstructed, in order to preserve the integrity of the audit trail, and ensure accountability for each processing operation and decision taken).

[29] Software enabling the ETIAS Central Unit and the ETIAS National Units to process applications and to manage consultations with other ETIAS National Units.

15. Conclusions

78. In light of the above, the EDPS makes the following recommendations:

(1) to strictly limit the purposes in Article 32(2) of the Proposal that could justify processing of personal data of individuals outside of the categories of data subjects listed in Annex II;

(2) to lay down clear maximum time limits on processing of uncategorised personal data in order avoid situations where personal data of individuals with no link to any criminal activity is retained in police databases for an extensive period of time;

(3) to define the criteria, based on which Europol would decide whether the processing of personal data of individuals outside of the categories of data subjects listed in Annex II, is 'relevant and necessary', either in the Regulation itself, or in a Management Board Decision after consultation with the EDPS;

(4) to specify the respective roles and data protection responsibilities, as well as the specific requirements applying to the processing of different categories of personal data during the access and use of Europol services and data processing tools referred to under Section II of Chapter III of the Proposal by other Union or Member States bodies. If not specified in the Europol Regulation itself, this aspect should at least be defined in respective implementing acts envisaged in the Proposal;

(5) to define in the Regulation, even if only in a general manner, the categories of personal data that would be included in the index(es) of the hit/no hit system laid down in Article 80 of the Proposal, which could then be further specified in the implementing act provided for in Article 80(9)) of the Proposal;

(6) to make publicly available and keep up to date an overview of all the Union and Member States authorities that would have indirect access to Europol systems;

(7) to clarify the meaning and the content of 'multimedia data' that could be used to query Europol systems pursuant to Articles 39(2)(c) and 41(2)(c) of the Proposal;

(8) to provide for a mandatory case-by-case assessment of both the necessity and proportionality of a query of the Europol Analytical Environment using biometric data processed for the purpose of uniquely identifying a natural person, and to amend accordingly Recital 106 of the Proposal;

(9) to maintain in Article 96 of the Proposal the logic of Article 26(2) of the current Europol Regulation, according to which Europol may as a rule process data received from private parties first and foremost in order to identify the Member State concerned. Derogations, i.e. processing for purposes that go beyond the purpose of identifying the Member State(s) having jurisdiction in the case, should only be allowed in specific circumstances that should be clearly circumscribed in the Proposal;

(10) to lay down in the substantive chapters of the Proposal consistently clear rules setting out the procedures, conditions and the specific safeguards applicable to the exercise of the various tasks entrusted to Europol and their related personal data processing activities. Moreover, the Proposal should cross-reference each of the tasks of the Agency laid down in Article 6 with the corresponding specific provisions / chapters governing the respective activity;

(11) to lay down in the Proposal a clear allocation of responsibility as regards the processing of personal data. If not specified in the Europol Regulation itself, the respective roles in multi-actor processing operations to be at least be defined in the dedicated implementing acts;

(12) to include in the Proposal a provision expressly granting the EDPS the power to supervise the data processing activities carried out by Europol staff embedded within national investigative environments, in particular though the establishment of Europol Support Offices;

(13) to extend in Article 113(4) of the Proposal the maximum deadline for national supervisory authorities to respond to consultation by the EDPS from three to six months and to introduce a presumption of agreement where a national supervisory authority does not deliver its opinion within the deadline set by the EDPS;

(14) to align the time limits for prior consultations in Article 108(1) of the Proposal with the timeline provided for in Article 90(4) EUDPR;

(15) to ensure that all providers of personal data to Europol are notified about data breaches concerning data they have provided, in all cases and without undue delay;

(16) to maintain and make available to the EDPS an up-to-date catalogue of all services and tools offered by Europol and the purposes for which they may be used;

(17) to ensure that, in addition to complying with Article 91 EUDPR, Europol is required to establish and maintain appropriate security governance documentation and procedures, including security and data protection risk assessments, security plans, business continuity plans and disaster recovery plans, covering all systems, infrastructures and interoperability components involved in the processing of operational data;

(18) to provide safeguards for traceability and accountability for each processing operation and decision taken in the ETIAS framework;

(19) to allocate additional human and financial resources to the EDPS, corresponding to the substantial expansion of Europol's tasks and data-processing capabilities.

Brussels, 11 August 2026

(e-signed)
Wojciech Rafał WIEWIÓROWSKI