



EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data
protection authority

Opinion 19/2026

on the Proposal for the Regulation on
the establishment of Eurojust and
repealing Regulation (EU) 2018/1727

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 establishment of the European Union Agency for Criminal Justice Cooperation (Eurojust) and repealing Regulation (EU) 2018/1727¹.

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) 570 final.

Executive Summary

On 24 June 2026, the European Commission adopted the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the European Union Agency for Criminal Justice Cooperation (Eurojust) and repealing Regulation (EU) 2018/1727.

The Proposal aims to improve Eurojust's internal functioning, governance, and operational performance as well as to expand Eurojust's mandate to cover emerging crime areas such as cybercrime, gender-based violence, and violations of EU restrictive measures, and to reinforce its analytical and proactive capabilities.

The EDPS supports the aim of the Proposal to streamline data protection rules for operational personal data processed by Eurojust, by identifying all common denominators of data protection rules applicable to Eurojust and regrouping them in Regulation (EU) 2018/1725 (EUDPR), thereby removing fragmentation and duplication. At the same time, the EDPS notes that the proposed extension of Eurojust's tasks would entail more complex processing operations, additional information flows, increased exchanges with national authorities and potentially third countries.

The EDPS welcomes that the Proposal maintains the principle that any automated processing of operational personal data should take place within the integrated data processing environment of the Case Management System (CMS), subject to limited exceptions. Similarly, the EDPS welcomes the clear obligation that communication between the competent national authorities and Eurojust should continue to primarily take place through a network of IT systems and interoperable e-CODEX access points, which would enable a secure and reliable cross-border exchange of information. The EDPS also welcomes the important data protection safeguards maintained in Chapter IV of the Proposal.

While noting all these positive elements, this Opinion also contains a number of specific recommendations with a view of ensuring appropriate level of data protection. In particular, the EDPS recommends defining, in a comprehensive manner, the roles and responsibilities of Eurojust and Member States when processing operational personal data. In addition, the EDPS considers that the Proposal should make explicit the elements allowing to clearly circumscribe which databases would Eurojust be allowed to cross-check and under which conditions. The EDPS also suggests making publicly available and keeping up to date an overview of EU bodies, offices and agencies that would have indirect access via Eurojust's "hit/no-hit" system.

Furthermore, circumstances in which Eurojust may exchange information with private parties should be clarified and appropriate safeguards for any exchange of personal data should be in place. Similar considerations apply where alternative means of communications are used or when making use of cloud computing. The EDPS also calls for clarifications of the rules applicable to international transfers and for updating of cooperation agreements and working arrangements concluded by Eurojust under Decision 2002/187/JHA or Regulation (EU) 2018/1727. Finally, the Opinion also underlines the need for additional allocation of both human and financial resources to the EDPS.

Contents

1. Introduction.....	4
2. General remarks	5
3. Cross-checking of information by Eurojust	6
4. Alternative means for the exchange of information	8
5. Case Management System (CMS)	8
6. Processing of operational personal data	9
7. Storage limits for discontinued criminal investigations..	10
8. Information security and cloud computing	10
9. Responsibility in data protection matters	11
10. Indirect information exchange on the basis of a hit/no-hit system.....	12
11. Strategic analysis.....	13
12. Exchange of operational personal data with the competent authorities of a third country	13
13. Legacy cooperation agreements and working arrangements with third countries	16
14. Exchange of data with private parties.....	16
15. Conclusions.....	17

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 adopted the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the European Union Agency for Criminal Justice Cooperation (Eurojust) and repealing Regulation (EU) 2018/1727³ ('the Proposal').
2. The objective of the Proposal is to address the shortcomings identified by the 2025 evaluation of Eurojust⁴ and to modernise Eurojust's legal framework in line with the Lisbon Treaty and the Common Approach on EU decentralised agencies. The Proposal aims to improve Eurojust's internal functioning, governance, and operational performance, while strengthening its cooperation with EU partners and third countries. In addition, the Proposal seeks to expand Eurojust's mandate to cover emerging crime areas such as cybercrime, gender-based violence, and violations of EU restrictive measures, including where they present a hybrid dimension, and to reinforce its analytical and proactive capabilities⁵.
3. The Proposal is part of a package of criminal justice initiatives aimed at strengthening the Union's capacity to prevent, detect, investigate and prosecute serious cross-border crime and was adopted together and in complementarity with the revisions of the Europol Regulation⁶, the European Investigation Order (EIO) Directive⁷ and the EUDPR⁸. The EDPS will issue separate opinions on each of these other 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

² OJ L 295, 21.11.2018, p. 39.

³ COM(2026) 570 final.

⁴ See SWD(2025) 182 final. The evaluation identified significant structural and operational constraints that impede its ability to fully realise its potential. According to the evaluation, these constraints include inefficiencies in internal governance, inconsistencies in the application of the Regulation across Member States, and limitations on cooperation with EU partners and third countries.

⁵ COM(2026) 570 final, p. 1.

⁶ See COM(2026) 580 final.

⁷ See COM(2026) 313 final.

⁸ See COM(2026) 314 final.

reference to this consultation in Recital 60 of the Proposal. The EDPS also positively notes that he was already previously informally consulted pursuant to recital 60 of EUDPR.

2. General remarks

5. The EDPS welcomes that the Proposal aims to respond to the evolving challenges posed by serious and organised cross-border crime in the European Union. While maintaining the management and operation elements that have proven efficient, it would modernise Eurojust's legal framework and streamline its functioning and structure⁹.
6. The EDPS highlights that the Proposal would significantly expand the scope of Eurojust's mandate. In addition to its existing areas of competence, Eurojust's revised mandate would cover several new crime areas: cybercrime, gender-based violence, crime of aggression and violations of EU restrictive measures¹⁰. The Proposal would also reinforce Eurojust's analytical and proactive capabilities, in particular Eurojust's operational activities on its own initiative¹¹. Additionally, the Proposal seeks to enable Eurojust to assist with investigations and prosecutions affecting two or more third countries or international organisations, where the case may have repercussions at Union level¹², as well as investigations and prosecutions affecting at least one Member State and a third country or an international organisation provided that a contact point has been designated in that third country or international organisation¹³.
7. The EDPS welcomes that the Proposal maintains the principle that any automated processing of operational personal data should take place within the integrated data processing environment of the Case Management System (CMS), subject to limited exceptions¹⁴. Similarly, the EDPS supports the clear obligation that communication between the competent national authorities and Eurojust should continue to primarily take place through a network of IT systems and interoperable e-CODEX access points, which would enable a secure and reliable cross-border exchange of information¹⁵.
8. The EDPS also welcomes Chapter IV, which maintains important data protection safeguards, in particular by defining the categories of operational personal data that Eurojust may process. This includes data on suspects, convicted persons, victims and other parties to proceedings. It also lays down strict time limits for the storage of operational personal data after the termination of a proceedings¹⁶, as well as specific data subject's rights regarding access to operational personal data processed by Eurojust.
9. The EDPS also positively notes that the Proposal aims to support the goal of streamlining data protection rules for operational personal data across EU agencies and bodies, including Eurojust. It clarifies that both the Eurojust Regulation and the EUDPR apply to Eurojust's data processing activities, with the specific data protection rules in the Eurojust Regulation

⁹ See COM(2026) 570 final, Explanatory Memorandum, p. 2.

¹⁰ See Annex I of the Proposal.

¹¹ See Chapter III, Section II.

¹² See Art 5(6)(d).

¹³ See Article 5(6)(c)(ii).

¹⁴ For more detail, see Section 5.

¹⁵ For more detail, see Section 4.

¹⁶ For more detail, see Section 7.

taking precedence (as *lex specialis*) over the EUDPR¹⁷. The EDPS understands that, with this Proposal, most of the data protection provisions are removed from the Eurojust Regulation with a view to avoiding duplication, since the corresponding rules are already set out in the EUDPR¹⁸, as the overarching data protection legislation for EU Institutions, bodies and agencies. The EDPS welcomes and fully supports the proposed direct application of the horizontal rules in Chapter IX of EUDPR to the processing of operational personal data by Eurojust. This is an important step towards a comprehensive alignment of the data protection framework for the EU institutions, offices, bodies and agencies active in the area of freedom, security and justice, which the EDPS has repeatedly called for¹⁹.

10. It should also be noted that the proposed extension of Eurojust's tasks would not only entail a quantitative increase in the volume of personal data processed. It would also likely involve more complex processing operations, additional information flows, increased exchanges with national authorities and potentially third countries, as well as a greater need to assess compliance with the applicable data protection safeguards. In this respect, the EDPS emphasises that information shared with Eurojust should clearly specify the purposes for which it may subsequently be processed. Any further processing of operational personal data should comply with the purpose limitation principle and be subject to a necessity and proportionality assessment. These developments would inevitably require more intensive and specialised supervision by the EDPS.
11. Effective supervision cannot be ensured without adequate resources. The EDPS' supervisory responsibilities over Eurojust are a necessary counterpart to the expansion of Eurojust's operational powers. If Eurojust is entrusted with additional tasks involving the processing of personal data, the EDPS must be equipped with the corresponding human and financial resources to exercise its supervisory mandate effectively, independently and in a timely manner. The EDPS therefore underlines the need for an additional allocation of both human and financial resources to the EDPS.
12. 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.

3. Cross-checking of information by Eurojust

13. According to recital 25 of the Proposal, one of the main challenges in combating serious cross-border crime is the timely identification of links and overlaps between ongoing investigations and prosecutions of criminal networks, in particular transnational organised crime networks involved in drug trafficking, and investigations and prosecutions concerning financial or other forms of serious fraud. Cross-checking of relevant information helps

¹⁷ See Art 43 of the Proposal and COM(2026) 570 final, Explanatory Memorandum, p. 12 as well as Recital 11 EUDPR.

¹⁸ For example, rules on onward transfers of personal data.

¹⁹ See, for instance, [EDPS Opinion 4/2021 on the Proposal for Amendment of the Europol Regulation](#), issued on 8 March 2021, para 40. The EDPS notes the Proposal for the revision of the EUDPR aims to identify all common denominators of data protection rules applicable to Europol and Eurojust, and regroups them in the EUDPR, thereby removing fragmentation and duplication. This will allow the founding acts of Union bodies, offices, and agencies active in the area of law enforcement and criminal justice to maintain only those tailored-made data protection rules, developed to reflect their respective specific operational needs and nature. See COM(2026) 314 final, p. 4.

promoting the efficiency of judicial administration by preventing the duplication of parallel proceedings before different national courts, thereby reducing the risk of violating the *ne bis in idem* principle.

14. Against this background, the Proposal tasks Eurojust²⁰ with cross-checking information stored in relevant databases to identify links between cross-border investigations and inform the Member States concerned, or where appropriate, the European Public Prosecutor's Office (EPPO), thereof and to support cross-border investigations²¹. This task is further mentioned in Article 28(2)(e) of the Proposal which allows National Members to ask the competent authorities of their Member States to authorise cross-checking of their relevant national databases, when Eurojust acts on its own initiative. In addition, Article 41(2)(e) provides that the Eurojust CMS shall serve the purpose of enabling the analysis and systematic cross-checking of information.
15. The EDPS recognises that cross-checking is necessary for Eurojust to fulfil its overall objective of supporting and strengthening coordination and cooperation between national investigating and prosecuting authorities in relation to serious cross-border crime. Nevertheless, in accordance with the principles of data minimisation and purpose limitation such cross-checking should remain limited to what is necessary and proportionate. In other words, the cross-checking of "relevant databases" mentioned in Articles 4 and 25 should be clearly delineated and not left as an open-ended clause.
16. The EDPS understands from the Proposal that Eurojust's cross-checking capabilities depend on the access rights of the National Members in charge of this cross checking. The EDPS notes that, in addition to the Eurojust's systems to which all National Members have access, the full scope of this "cross-checking of relevant databases" would depend on the access rights granted by a particular Member State's law to their National Member regarding their national information systems²². The EDPS also understands that no cross-checking of EU data bases (other than the Eurojust ones) is envisaged under Articles 4 and 25 of the Proposal.
17. The EDPS recommends that, before any cross-checking of personal data against national information systems is carried out, National Members should ensure that such further processing is (a) necessary and proportionate in light of the intended purpose; (b) authorised by the owner/provider of the personal data; (c) in accordance with the Member State law governing access to the national information.
18. Furthermore, the EDPS recommends making these elements explicit in Articles 4 and 25 as well as in Recital 25, in order to clearly circumscribe which databases would Eurojust (through National Members) be allowed to cross-check and under which conditions.

²⁰ See Articles 4(c) and 25(2)(e).

²¹ Recital (25) further indicates that Eurojust should cross-check information stored in the relevant databases 'systematically'.

²² See to that effect Article 18(6) and Article 28(2)(e).

4. Alternative means for the exchange of information

19. The EDPS understands that the communication between the competent national authorities and Eurojust under the Proposal will primarily take place through a network of IT systems and interoperable e-CODEX access points ('the decentralised IT system'). The Eurojust CMS will be connected to this decentralised IT system²³. The EDPS welcomes the usage of this system, which would enable a secure and reliable cross-border exchange of information.
20. Article 40(2) of the Proposal, nevertheless, provides for the possibility of alternative means for the exchange of information where exchange of information via the decentralised IT system is not possible due to, for instance, the unavailability of the system, the nature of the transmitted material, technical limitations, such as data size, legal constraints relating to the admissibility as evidence of the requested data or to forensic requirements applicable to the requested data, or exceptional circumstances.
21. The EDPS does not object that, in such exceptional circumstances, the transmission be carried out by other appropriate alternative means. However, the provision should expressly require the implementation of measures guaranteeing a substantially equivalent level of confidentiality and integrity of information exchanged through alternative means as for the decentralised IT system.

5. Case Management System (CMS)

22. Article 41(1) of the Proposal requires Eurojust to establish a case management system for the processing of operational personal data listed in Annex II, data listed in Annex III and non-personal data.
23. The EDPS welcomes the clear indication in paragraph (6), that Eurojust must not carry out any automated processing of operational personal data outside the integrated data processing environment of the CMS, except in limited cases explicitly provided for under the Proposal. This constitutes an important guarantee that personal data will be held in a secure and controlled environment.
24. The same paragraph provides for an exception, by allowing National Members to temporarily store and analyse personal data for the purpose of determining whether such data are relevant to Eurojust's tasks and whether a case should be opened in the case management system. Those data may be held for a period not exceeding six months, which may be extended once for a further period not exceeding six months in cases where the National Member has – exceptionally – not been able to make that determination. The EDPS welcomes that, for these situations, the Proposal obliges Eurojust to still hold those data in a secure and controlled environment provided by Eurojust for this purpose, subject to appropriate safeguards substantially equivalent to those identified for the case management system.

²³ Article 40(1) of the Proposal.

25. The EDPS recommends, however, introducing the obligation to properly justify any extension of the deadline of six months for the storage of operational personal data outside the integrated processing environment of the case management system. The same recommendation applies to Article 28(6) of the Proposal, allowing authorised Eurojust staff to temporarily store and analyse personal data in the CMS for the purpose of enabling the National Member or the College to determine whether such data are relevant to Eurojust's tasks and whether a case should be opened in the CMS.
26. Another exception is provided in paragraph (7), for cases where Eurojust is authorised to process operational or non-operational personal data 'but does not act as controller in respect of such data'. The EDPS recommends that, for that separate system, there should be a requirement of the same level of protection (i.e. safeguards substantially equivalent to those ensured by Eurojust when it is acting as a controller). In addition, the EDPS recommends clarifying what would be the role of Eurojust in cases when it 'does not act as a controller'²⁴.
27. The EDPS also notes the statement in Article 41(8): 'In the performance of their tasks, National Members may process personal data on the individual cases on which they are working, in accordance with this Regulation or other applicable instruments.' The EDPS understands that the "performance of their tasks" refers to National Members performing Eurojust's tasks and therefore suggests, for the sake of clarity, to explain that, for these tasks, personal data shall be processed in accordance with the provisions of the Eurojust Regulation and the EUDPR. In case "performance of their tasks" should also encompass processing of personal data on a purely national level, this should then be further explained and reflected in the Proposal.
28. Finally, the EDPS recalls that the CMS should be designed, developed and operated based on a documented security and data protection risk assessment and an associated plan for relevant measures²⁵.

6. Processing of operational personal data

29. The EDPS notes Article 44(3) of the Proposal, which enables Eurojust to process operational personal data other than the personal data referred to in Annex II. The EDPS understands that there may be situations where there would be operational need to process additional data immediately relevant to ongoing coordinated investigations. However, the EDPS considers that these situations need to be clearly circumscribed.
30. In that regard, the EDPS welcomes that this provision retains²⁶ important data protection safeguards for such processing, by specifying that it may take place only 'in exceptional cases, for a limited period of time which shall not exceed the time needed for the conclusion of the case in relation to which the data are processed [...] where such data are immediately relevant to and are included in ongoing investigations which Eurojust is coordinating or

²⁴ See further Section 9 of the Opinion.

²⁵ See also Section 8 of the Opinion.

²⁶ See Article 27(3) of Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA (OJ L 295, 21.11.2018, pp. 138).

helping to coordinate [...]’ and ‘the Data Protection Officer[...] shall be informed immediately [...] and shall be informed of the specific circumstances which justify the necessity of the processing of those operational personal data. Where such other data refer to witnesses or victims [...] the decision to process them shall be taken jointly by the National Members concerned.’

7. Storage limits for discontinued criminal investigations

31. The EDPS welcomes Article 45 of the Proposal which provides for time limits for the storage of operational personal data. The EDPS reminds that, in line with the CJEU case law²⁷, the determination of a storage duration must be based on objective criteria. Different storage duration should be set for the different categories of data stored ‘on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned’²⁸.
32. In that regard, while taking note of the different time limits that are already set, the EDPS considers an additional storage limit should be determined in Article 45(1) for cases where prosecutors decide to discontinue a criminal investigation and not to prosecute a certain offence before the case even comes to court, similarly to what is already provided for in paragraph 2(b) of the same Article²⁹.

8. Information security and cloud computing

33. Article 46 of the Proposal requires Eurojust and Member States to define mechanisms to ensure that the security measures referred to in Article 91 EUDPR are addressed across information system boundaries.
34. The EDPS recommends that this Article explicitly requires that Eurojust, in addition to complying with Article 91 EUDPR, establishes and maintains 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.

²⁷ Judgment of the European Court of Justice of 8 April 2014, *Digital Rights Ireland and Seitlinger and others*, C-293/12 and C-594/12, EU:C:2014:238, note 2, par. 64.

²⁸ *Idem*, note 2, par. 63.

²⁹ The time limit included in Article 45(2)(b), however, refers only to operational personal data transmitted in accordance with Article 38 (information provided by Eurojust by national authorities). It does not address operational personal data processed by Eurojust in general, for the performance of its tasks.

35. In addition, the EDPS recalls the obligation of Eurojust (as an EU body) to appoint a local cybersecurity officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity³⁰.
36. According to Article 40 (7) of the Proposal, '[w]here Eurojust establishes or procures cloud computing services for the purposes of this Regulation, it shall ensure that such services comply with applicable Union law, including requirements on the EU cloud sovereignty framework, data security, data protection, cybersecurity and digital sovereignty, thereby ensuring the secure hosting and processing of data exchanged under this Regulation, with strict access control and data compartmentalisation'.
37. In this context the EDPS observes that, pursuant to Article 30(3) of 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"), 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 must have a Union assurance level 2, 3 or 4³¹. However, according to paragraph 4 of the same Article, in certain cases, the assurance level could be further lowered to level 1, including for financial reasons.
38. The personal data collected for justice and 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.
39. In the light of the above, the EDPS considers that the cloud computing services procured by Eurojust should meet the highest Union assurance levels (preferably level 4 but in any event not lower than level 3).

9. Responsibility in data protection matters

40. The EDPS understands that Article 53 of Proposal aims to clarify the responsibilities of Eurojust when it comes to processing of both operational and administrative personal data. It assigns the responsibility to Eurojust for compliance with the EUDPR in relation to administrative personal data and for compliance with the Eurojust Regulation and with EUDPR in relation to operational personal data which it would process. In addition, the Proposal allocates the responsibilities of Eurojust and Member States as regards certain obligations under data protection law (such as accuracy and lawfulness of transmission).

³⁰ See Article 6(8) of Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ L, 2023/2841, 18.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2841/oj>)

³¹ Level 1 being the least secure and level 4 the most secure.

41. Article 53, however, does not expressly clarify the role of Eurojust under data protection law (i.e. as controller, joint controller or processor) in relation to the different processing activities it carries out.
42. The EDPS considers that a clear definition of the 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 affects the effective exercise of data subjects' rights³².
43. The EDPS therefore recommends defining the roles and responsibilities of Eurojust and Member States in a comprehensive manner, including by specifying that Eurojust would be the controller for the processing of personal data within the systems managed by Eurojust such as the CMS and the hit/no-hit system. In addition, the EDPS recalls that any relationship between (joint) controllers and processors must be governed by appropriate legal arrangements³³. 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.

10. Indirect information exchange on the basis of a hit/no-hit system

44. Article 55(1) of the Proposal requires Eurojust to take all appropriate measures to ensure indirect access by other Union bodies, offices and agencies, 'where such access is provided for in Union law', to information held by Eurojust, under conditions of reciprocity, by means of an automated hit/no-hit system operated through the searching of indexes which shall be kept up to date.
45. While the EDPS welcomes the express clarification that the access by other EUIs must be 'provided for in Union law', the EDPS notes that the Proposal does not provide a comprehensive overview of all EU bodies, offices and agencies that may have such access (now or in the future). In the interest of transparency, the EDPS recommends requiring Eurojust to make publicly available and keep up to date an overview of EU bodies, offices and agencies that would have such indirect access.
46. The EDPS also welcomes, in paragraph (3) of the same Article, the detailed explanation of the actions that follow in case of a hit. However, the EDPS suggests clarifying whether any answer would be given to the requesting Union body, office or agency in case there would be no hit or in cases where there would be a hit, but the information would be subject to restrictions and the provider of the information would maintain those restrictions, even after

³² See [EDPS Guidance for co-legislators on key elements of legislative proposals](#), issued on 7 May 2025, para 25-26. See in the same vein also Recital 36 of the Proposal ("The protection of the rights and freedoms of data subjects requires a clear attribution of responsibilities for data protection under this regulation").

³³ See also [EDPS Guidance for co-legislators on key elements of legislative proposals](#), issued on 7 May 2025, para 28-35.

being contacted by Eurojust³⁴. The EDPS would like to underline that, in the latter situations, there should be no disclosure of the fact that there was a hit.

47. The Proposal should additionally specify, even if only in a general manner, the categories of personal data to be included in the index of the system, which could then be further specified in the implementing act provided for in Article 55(8) of the Proposal.
48. When it comes to the implementing acts, the EDPS also reminds that they should fully consider the principle of data protection by design and by default and that the development, implementation and operation of the system, including any system-to-system connections should be subject to a mandatory prior consultation of the EDPS (in addition to the mandatory consultation on the implementing act pursuant to Article 42(1) EUDPR). Additionally, the requirements for a 'hit' to be considered successful should be clearly set out.

11. Strategic analysis

49. The Proposal aims to expand Eurojust's analytical and strategic functions³⁵. In that regard, Recital 35 of the Proposal explains that 'the Regulation provides for the possibility of retaining operational personal data for a longer period where strictly necessary for analytical and strategic purposes, subject to clear conditions and robust data protection safeguards, and within a clear and legally certain framework consistent with the applicable Union data protection rules'.
50. While the EDPS understands that the possibility of retaining operational personal data for a longer period would be provided for in Article 45(4) and (8) of the Proposal, it is not clear to which 'robust data protection safeguards' does Recital 35 refer to, as no corresponding provision is to be found in the enacting terms. The legislation providing for the interference with the fundamental right to protection of personal data must directly and specifically provide the required safeguards, especially where the link between the processing of personal data and the purpose to be achieved is less direct, as is the case for strategic analysis. The EDPS therefore recommends clarifying the safeguards in the Proposal.

12. Exchange of operational personal data with the competent authorities of a third country

51. As a preliminary and overarching remark, the EDPS recalls that Eurojust is an agency of the Union. All processing of operational personal data by Eurojust — including processing carried out by National Members acting within the structure of Eurojust and by Liaison

³⁴ In case of a hit with restrictions maintained, it should be clarified whether there would a) be a confirmation of a hit by Eurojust but no sharing of (restricted) information b) there would simply be no return of a hit (the system would 'stay silent') or c) the system would return a 'no hit' feedback. Similarly, for 'no hit' situations it should be clarified whether the system would 'stay silent' or it would give a 'no hit' feedback.

³⁵ See Recital (7) and Articles 30-31 and Article 34 of the Proposal.

Officers, who are members of Eurojust staff³⁶ — is governed exclusively by the Eurojust Regulation and by EUDPR. Consequently, transfers of operational personal data by Eurojust to third countries or international organisations may take place only under the conditions laid down in Articles 94b, 94c and 94d of the EUDPR. Neither national law nor international commitments entered into by a Member State can constitute a legal basis for such transfers.

52. Any provision that would permit transfers of operational personal data processed by Eurojust on a basis other than the EUDPR would create a parallel transfer channel circumventing the rules and safeguards that EU data protection law established specifically for Union institutions, bodies, offices and agencies. Such circumvention would (i) interrupt the continuity of protection that must accompany personal data when it leaves the Union, contrary to the requirement of an essentially equivalent level of protection established by the Court of Justice³⁷; (ii) fragment the level of protection afforded to data held in Eurojust's CMS, which would then vary according to the Member State of the authorising National Member; (iii) dissociate the transfer decision from Eurojust's responsibility as controller under the accountability principle; and (iv) remove such transfers from the supervision of the EDPS, without any national supervisory authority being competent to supervise Eurojust's processing in its place, thereby creating a supervisory gap.
53. Against this background, the EDPS notes with concern that Article 18(1)(c) grants National Members the power to directly 'exchange operational information and evidence with competent national authorities of third countries and competent organs of international organisations, in accordance with the international commitments of their Member State and in accordance with data protection rules'.
54. The reference to 'data protection rules' in this Article does not specify which rules are meant. If the provision were read as allowing the international commitments of a Member State to serve as the basis for a transfer of operational personal data processed by Eurojust, subject only to unspecified data protection rules, it would establish a parallel legal basis for transfers alongside the EUDPR, with the consequences described above. The EDPS recalls that an international commitment of a Member State is not among the legal bases on which Eurojust may transfer operational personal data to a third country or an international organisation. The EDPS therefore recommends clarifying in Article 18(1)(c) that, insofar as the exchange concerns operational personal data processed by Eurojust, it may take place exclusively in accordance with Articles 94b, 94c and 94d of the EUDPR. International commitments of the Member State concerned may govern the judicial cooperation dimension of the exchange, but cannot substitute for, or derogate from, the transfer regime of the EUDPR.
55. Article 18(1)(e) further grants National Members the power to 'authorise, on the basis of all relevant information available, including, where appropriate, input from the Data Protection Officer, the transfer of operational personal data necessary for the purposes of a specific investigation in which their Member State is involved, in accordance with Articles 94b, 94c and 94d of Regulation (EU) 2018/1725'.

³⁶ See Article 61(2) of the Proposal.

³⁷ See, by analogy, Judgment of the Court of Justice of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, in particular paragraphs 93 to 96 and 105; see also Opinion of the Court of Justice 1/15 of 26 July 2017, EU–Canada PNR Agreement EU:C:2017:592, paragraph 214.

56. The EDPS welcomes the express reference to Articles 94b, 94c and 94d of the EUDPR. However, the words ‘where appropriate’ render the involvement of the Data Protection Officer discretionary. The assessment of whether appropriate safeguards exist in a specific case, or of whether and on what basis a derogation may be relied upon, requires specialised data protection expertise. Systematic consultation of the Data Protection Officer would ensure that such assessments are conducted in a consistent and objective manner across Eurojust. The EDPS therefore recommends deleting the words ‘where appropriate’ in Article 18(1)(e), so that the authorisation of any such transfer of operational personal data is always preceded by input from the Data Protection Officer.
57. The EDPS notes that Article 61(3) of the Proposal allows Eurojust’s Liaison Officers posted to third countries, if authorised by National Members³⁸ and under their supervision and responsibility, to exchange operational personal data directly with the competent authorities of a third country. As recalled in paragraph 51 of this Opinion, Liaison Officers are members of Eurojust staff. Therefore, any transfer of operational personal data by a Eurojust Liaison Officer to competent authorities of a third country needs to follow the rules and safeguards applicable to international transfers as established under the EUDPR. Introducing transfers based solely on an authorisation by a National Member would circumvent the applicable safeguards under the EUDPR and would risk exposing the data to transfers without adequate levels of protection that were not subject to the necessary legal and data protection assessments.
58. The EDPS also notes the discrepancy between Article 18(1)(e), which expressly conditions the National Member’s authorisation on compliance with Articles 94b, 94c and 94d of the EUDPR, and Article 61(3), which contains no such reference. The EDPS therefore recommends aligning Article 61(3) with Articles 18(1)(e) and 63(5) of the Proposal, by clarifying that any exchange of operational personal data under Article 61(3) may take place exclusively in accordance with the EUDPR.
59. The EDPS furthermore notes that the Proposal introduces contact points of third countries to be hosted at Eurojust³⁹, with direct access to the CMS. This leads to the situation where an international transfer of operational personal data can be performed by a National Member simply granting access in the CMS to a contact point of a third country⁴⁰. While the EDPS recognises this may be beneficial for operational efficiency, the inherent risks associated with such an approach and the need for appropriate safeguards and policies to ensure the effective application of the rules governing international transfers should also be acknowledged.
60. In that regard, the EDPS notes that Article 62(4), dealing with liaison prosecutors posted at Eurojust, clearly states that ‘[t]ransfers of operational personal data to liaison prosecutors through the case management system shall take place only in compliance with this Regulation and Regulation (EU) 2018/1725’. While recognising that Article 63(5) already provides that any exchange of operational personal data must be in accordance with the EUDPR, for reasons of consistency, the EDPS suggests aligning the wording of Article 63(5) with the wording of Article 62(4) of the Proposal.

³⁸ Where such exchanges involve the Member State of that National Member.

³⁹ See Article 63 (5) of the Proposal.

⁴⁰ See Article 42(2)(d) of the Proposal.

61. To ensure further clarity, Articles 42(2) (b) and (d) should be supplemented by referencing Article 18(1)(e), to emphasise that such access by liaison officers and contact points represents an international transfer and should be authorized only where necessary for the purposes of a specific investigation in which the Member State of the National Member is involved and after consulting the Data Protection Officer⁴¹.
62. Finally, the EDPS notes that the scope of Article 54(2) has been expanded to allow Eurojust to exchange directly any information, including administrative personal data, with Union institutions, bodies, offices and agencies and with the competent authorities of third countries and international organisations. The EDPS suggests that it is made clear that any exchange of personal data has to be done in accordance with the applicable data protection rules and, in this specific case, in accordance with the EUDPR provisions governing the processing of administrative personal data.

13. Legacy cooperation agreements and working arrangements with third countries

63. Article 86(8) of the Proposal mentions that the Proposal shall not affect the validity of cooperation agreements and working arrangements concluded by Eurojust under Decision 2002/187/JHA or Regulation (EU) 2018/1727. Such cooperation agreements and working arrangements will remain in force and shall be applied until they expire or are amended or replaced.
64. While recognising that not all legacy agreements and working arrangements can be revised and amended at once, the EDPS would like to remind that these instruments were negotiated prior to the entry in force of the current data protection legislation and their continued application should be conceived as temporary and adaptation-oriented from the outset, not as a perpetual exemption. The EDPS, therefore, recommends providing an obligation for the Commission to review all legacy agreements and working arrangements and, where needed, start the negotiations of new agreements, thus ensuring the alignment of the agreements previously concluded by Eurojust with the current EU data protection legal framework.

14. Exchange of data with private parties

65. The EDPS notes that the Proposal includes the possibility for Eurojust to exchange information, including operational personal data, with “relevant private parties”⁴².

⁴¹ On the involvement of the Data Protection Officer, see also paragraph 56 of this Opinion.

⁴² See Article 4(b), Article 25(2)(b)(iii), Article 28(1), Article 29(3), Article 41(2)(d), Article 53(2)(c) of the Proposal.

66. In this regard, the EDPS recalls that while this would be a novelty for Eurojust, exchanges of personal data with private parties are an already established practice for other EU agencies in the area of justice and home affairs, such as Europol⁴³.
67. However, unlike Europol, the Proposal does not specify under which circumstances, conditions and safeguards such exchange would be allowed. In addition, the EDPS also notes that the Proposal, contrary to Europol Regulation⁴⁴, does not define the notion of ‘private parties’.
68. The EDPS therefore recommends defining the notion of ‘private parties’ and specifying explicitly in the Proposal in which cases and under which conditions and safeguards Eurojust would be allowed to exchange personal data with private parties.

15. Conclusions

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

- (1) To make explicit, in Articles 4 and 25 as well as in Recital 25, the elements allowing to clearly circumscribe which databases would Eurojust (through National Members) be allowed to cross-check and under which conditions.*
- (2) To require, in Article 40(2), the implementation of measures guaranteeing a substantially equivalent level of confidentiality and integrity of information exchanged through alternative means as for the decentralised IT system.*
- (3) In Articles 28(6) and 41(6), to introduce an obligation to properly justify the extension of the deadline of six months for storage of data.*
- (4) To require the same level of protection for the separate system mentioned in Article 41(7) and to clarify in this provision what would be the role of Eurojust in cases when it “does not act as a controller”.*
- (5) To clarify in Article 41(8) that personal data is to be processed by National Members in accordance with the provisions of the Eurojust Regulation and the EUDPR.*
- (6) To provide for, in Article 45(1), an additional storage limit for cases where prosecutors decide to discontinue a criminal investigation.*
- (7) To introduce, in Article 46, the requirement that Eurojust, in addition to complying with Article 91 EUDPR, establishes and maintains 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.*

⁴³ See Article 26 of 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, pp. 53).

⁴⁴ See Article 2(g) of Regulation (EU) 2016/794.

- (8) *To ensure that the cloud computing services, procured by Eurojust, meet the highest Union assurance level.*
- (9) *To define in a comprehensive manner the roles and responsibilities of Eurojust and Member States, including by specifying that Eurojust would be the controller for the processing of personal data within the systems managed by Eurojust - the CMS and the hit/no-hit system.*
- (10) *To require in Article 55 that Eurojust makes publicly available and keeps up to date an overview of the which EU bodies, offices and agencies have indirect access to information held by Eurojust.*
- (11) *To clarify in Article 55(3) whether any answer would be given to the requesting Union body, office or agency in cases there would be no hit or in cases where there would be a hit, but the information would be subject to restrictions.*
- (12) *To specify in Article 55, even if only in a general manner, the categories of personal data to be included in the index of the hit/no-hit system.*
- (13) *To clarify in one or more dedicated provisions to which “robust data protection safeguards” Recital 35 refers to.*
- (14) *To clarify in Article 18(1)(c) that, insofar as the exchange concerns operational personal data processed by Eurojust, it may take place exclusively in accordance with Articles 94b, 94c and 94d of the EUDPR.*
- (15) *To delete the words ‘where appropriate’ in Article 18(1)(e).*
- (16) *To align Article 61(3) with Articles 18(1)(e) and 63(5), by clarifying that any exchange of operational personal data under Article 61(3) may take place exclusively in accordance with the EUDPR.*
- (17) *To align the wording of Article 63(5) with the wording of Article 62(4).*
- (18) *To supplement Articles 42(2) (b) and (d) by referencing Article 18(1)(e).*
- (19) *To clarify in Article 54(2) that any exchange of personal data has to be done in accordance with the applicable data protection rules and, in this specific case, in accordance with the EUDPR provisions governing the processing of administrative personal data.*
- (20) *To provide for an obligation for the Commission to review all Eurojust’s legacy agreements and working arrangements and, where needed, start the negotiations of new ones fully aligned with the EU legal framework on data protection.*
- (21) *To define the notion of ‘private parties’ and to specify explicitly in the Proposal is which cases and under which conditions and safeguards Eurojust would be allowed to exchange personal data with private parties.*

Brussels, 11 August 2026

(e-signed)

Wojciech Rafał WIEWIÓROWSKI