EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Opinion 27/2026

on the Proposal on the signing and provisional application of the Framework Agreement between the European Union and the United States of America on the reciprocal exchange of information for identity verification, screening and vetting

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 Council Decision on the signing and provisional application of the Framework Agreement between the European Union and the United States of America on the reciprocal exchange of information for identity verification, and screening and vetting, relating to border procedures and applications for travel authorisations and visas, pursuant to Article 218 TFEU[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) 484 final.

Executive Summary

On 10 September 2026, the European Commission issued a Proposal for a Council Decision on the signing and provisional application of a Framework Agreement between the European Union and the United States of America (U.S.). The objective of the Framework Agreement is to set the conditions for the reciprocal exchange of information between the competent authorities of the EU Member States and of the U.S. for identity verification, screening and vetting of individuals in the context of border checks and applications for travel authorisations and visas necessary to determine whether the traveller's entry or stay would pose a serious and genuine risk to public security or public order. The Proposal is linked to the requirement by the U.S for admission to and further participation in the U.S. Visa Waiver Program, pursuant to which the partner countries have to conclude an 'Enhanced Border Security Partnership' ('EBSP') with the U.S. Department of Homeland Security.

The EDPS recalls that the Framework Agreement would be the first agreement concluded by the EU with a third country that implies large-scale sharing of personal data, including biometric data, for the purpose of border and immigration control. It is therefore of utmost importance to ensure that any processing of personal data pursuant to the Framework Agreement remains limited to what is strictly necessary and proportionate. With this objective in mind, this Opinion provides recommendations to ensure that the implementation of the Framework Agreement, and the subsequent bilateral agreements, comply with the requirements of proportionality, necessity and accountability.

In relation to the bilateral agreements, the EDPS underlines the importance of carefully designating the national information systems from which information is to be exchanged. The possible offences that could be considered as presenting risks to 'public order' and 'public security' should also by clearly specified, as well as the notion and parameters of the 'nexus' to a given country. Moreover, the Competent Authorities should carefully assess, on a case-by-case basis, whether the reason to believe that the entry or stay of an individual could pose a serious and genuine risk to public security or public order is based on objective material that establishes an objective link between the risk to public security or public order and the individual concerned. To enable this assessment, the Requesting Competent Authority should be required to indicate the specific reasons giving rise to the belief that a specific individual may pose a risk. In case there is a need for onward sharing, the Requested Competent Authority should be informed of such onward sharing in an effective manner.

The EDPS calls on the Commission to closely monitor whether judicial redress is available in practice for all data subjects, irrespective of their citizenship or nationality and to regularly assess the compliance with human rights obligations as a ground for possible suspension or termination of the Framework Agreement. The Opinion also recommends a number of additional practical arrangements, such as a requirement that before the start of the provisional application of the Framework Agreement, the U.S. side should formally notify the EU about its competent supervisory authorities, including their specific tasks and powers.

Contents

1. Introduction..... 4

2. General remarks 5

3. Material Scope 7

4. Individuals concerned..... 8

5. Criteria for determining the existence of risk..... 9

6. Justification of the query 11

7. Special categories of personal data..... 12

8. Purpose limitation and further processing 13

9. Onward sharing and transfers..... 14

10. Judicial and administrative redress..... 15

11. Effective oversight 16

12. Suspension and termination..... 16

13. 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 10 September 2026, the European Commission issued a Proposal for a Council Decision on the signing and provisional application of the Framework Agreement between the European Union and the United States of America on the reciprocal exchange of information for identity verification, and screening and vetting, relating to border procedures and applications for travel authorisations and visas, pursuant to Article 218 TFEU[3] ('the Proposal'), accompanied by an Annex containing the Framework Agreement[4].

2. The objective of the Proposal is to set the conditions for the reciprocal exchange of information, through a Framework Agreement, between the competent authorities of the EU Member States and of the United States of America ('U.S.') for identity verification, screening and vetting of individuals in the context of border checks and applications for travel authorisations and visas necessary to determine whether the traveller's entry or stay would pose a serious and genuine risk to public security or public order.

3. The Proposal is linked to the new requirement by the U.S. for admission to and further participation in the U.S. Visa Waiver Program ('VWP'), which enables citizens of participating countries to travel to the United States visa-free for maximum 90 days for the purpose of tourism or business[5]. It entails the conclusion of an 'Enhanced Border Security Partnership' ('EBSP') with the U.S. Department of Homeland Security ('DHS'). Consequently, the envisaged Framework Agreement would apply to those Member States which enjoy a visa free status with the U.S. or who wish to join the U.S. VWP[6].

4. Bilateral agreements between Member States and the U.S. will set out the specifics of the information exchange with the U.S. from their own national information systems,

[2] See OJ L 295, 21.11.2018, p. 39.
[3] See COM(2026) 484 final.
[4] COM(2026) 484 final Annex.
[5] See Explanatory Memorandum, COM(2026) 484 final, p. 1.
[6] See Explanatory Memorandum, COM(2026) 484 final, p. 2.

considering national legal requirements, the set-up of national databases, and other technical requirements or limitations[7].

5. As regards bilateral agreements already concluded by Member States with the U.S. prior to the entry into force of this Framework Agreement, the Framework Agreement includes the conditions under which such agreements remain applicable. In particular, the Framework Agreement would supplement, as appropriate, the relevant provisions regarding the protection of personal data in existing EBSPs.

6. The present Opinion of the EDPS is issued in response to a consultation by the European Commission of 10 September 2026, pursuant to Article 42(1) of EUDPR. The EDPS welcomes the reference to this consultation in Recital 11 of the Proposal.

2. General remarks

7. The conclusion of an EBSP with the U.S. Department of Homeland Security is a condition for admission to, and further participation in the U.S. VWP. The EBSP would complement the already existing traveller information exchange agreements such as the Agreements on Enhancing Cooperation in Preventing and Combating Serious Crime (PCSC Agreements), which establishes information exchange, including biometric data, on individuals who are suspected or convicted of terrorist offences or serious crime[8].

8. Given the review of the U.S. VWP and the deadline set by the U.S. to implement the EBSP requirement by end of 2026, the Commission proposes that the Framework Agreement should be applied on a provisional basis, in accordance with Article 32 thereof, as of its signature, pending the completion of the procedures necessary for its entry into force[9].

9. On 17 September 2025, the EDPS issued its Opinion 24/2025 on the negotiating mandate of this Framework Agreement, where it had the opportunity to examine the level of protection of fundamental rights and freedoms granted by the proposed agreement, as it would result if the negotiating directives were all fully implemented[10].

10. As already highlighted in the previous Opinion of the EDPS, the proposed Framework Agreement would set an important precedent, as it would be the first agreement concluded by the EU implying large-scale sharing of personal data, including biometric data, for the purpose of border and immigration control with a third country. In this context, the EDPS reaffirms the importance of establishing a common EU-U.S. framework for information exchange, in the context of the EBSP, that would set common Union-level conditions and safeguards, in order to ensure a high level of protection of the fundamental rights and freedoms[11].

---

[7] See Explanatory Memorandum, COM(2026) 484 final, p. 2.
[8] See Explanatory Memorandum, COM(2026) 484 final, p. 1 and 5.
[9] See Recital (7), COM(2026) 484 final.
[10] EDPS Opinion 24/2025 on the negotiating mandate for a framework agreement between the European Union and the United States of America on the exchange of information for security screenings and identity verifications, issued on 17 September 2025.
[11] EDPS Opinion 24/2025 on the negotiating mandate for a framework agreement between the European Union and the United States of America on the exchange of information for security screenings and identity verifications, issued on 17 September 2025, paragraph 9.

11. While the EDPS recognises the importance of ensuring border protection and security in the EU Member States and the U.S. , the EDPS stresses the critical importance of providing an adequate level of data protection and ensuring strict and effective implementation of the principles of necessity and proportionality in practice. In particular, the Framework Agreement and the subsequent bilateral EBSP agreements should prevent the exchange of personal data pertaining to individuals with no established links to serious and genuine threats to public security or public order.

12. While the EDPS acknowledges the time constraints for the negotiation, it nevertheless regrets the absence of an in-depth fundamental rights impact assessment accompanying the Proposal, given the seriousness of the interference resulting from the envisaged sharing of personal data for U.S. border and immigration control authorities.

13. The EDPS furthermore notes that due to the scope and purpose of the Proposal, the EU-U.S. 'Umbrella Agreement'[12] would not be applicable to the transfers envisaged by the U.S. under the EBSP, and, instead, the Framework Agreement aims to lay down the necessary adequate data protection and privacy safeguards for the transfers within the meaning of Union data protection law[13]. At the same time, the EDPS notes that the Framework Agreement does not constitute in itself the legal basis for any exchanges of personal data with the U.S, which would be provided for by the bilateral agreements[14].

14. In view of the above-described purpose and nature of the Framework Agreement, the EDPS emphasises the crucial role of the bilateral EBSP agreements between the EU Member States and the U.S. Even if their objective is to further specify the modalities of the information exchange[15], the effective implementation of the data protection safeguards will very much depend on the specific conditions laid down in the bilateral agreements negotiated by the EU Member States.

15. For instance, the choice of specific national information systems, from which information is to be exchanged under the Framework Agreement[16] will have a direct impact on the scope of the exchange of data. The same applies to the grounds for refusal the transfer, given that Article 11 of the Framework Agreement provides only an indicative list of such grounds. In addition, pursuant to Article 9(3), the bilateral agreements should specify the categories of personal data that may be exchanged. Regarding the latter, in line with its comments in the Opinion on the negotiating mandate, the EDPS regrets that the categories of personal data that may be exchanged as part of the additional information in the second step[17] are not described, even in a general manner, at the level of the Framework Agreement.

16. The EDPS also recalls its recommendation from the previous Opinion that any sharing of personal data from the EU large-scale IT systems in the area of justice and home affairs, in particular for border and migration control purposes, such as the Visa Information System (VIS) or the European Travel Information and Authorisation System (ETIAS), should be strictly excluded. In this regard, it positively notes that this important condition seems to

[12] Council Decision (EU) 2016/920 of 20 May 2016 on the signing, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, (OJ L 154, 11.6.2016 ELI: http://data.europa.eu/eli/dec/2016/920/oj).
[13] See Explanatory Memorandum, COM(2026) 484 final, p. 3.
[14] See Article 1(3) of the Annex to the Proposal, COM(2026) 484 final.
[15] See Article 5 of the Annex to the Proposal, COM(2026) 484 final.
[16] See Article 5(b), Annex to the Proposal, COM(2026) 484 final.
[17] See Article 9 of the Annex to the Proposal, COM(2026) 484 final.

be reflected, even if not explicitly, in Article 5 (b) of Framework Agreement, which refers only to national information systems with regard to the exchange of information[18]. Nevertheless, in view of the closed interconnectivity and interoperability of the Union and national IT systems in this area, the EDPS once again stresses the need for the Member States to prevent any possible indirect sharing of data from the EU large-scale IT systems in the area of justice and home affairs, in particular for border and migration control purposes.

17. This Opinion aims to provide constructive and objective advice with a view of ensuring that the implementation of Framework Agreement provides for the appropriate level of data protection, while delivering on its main policy objectives. In this context, the EDPS has focused, among others, on the purpose, material and personal scope and the envisaged data protection safeguards, including oversight and redress mechanisms, and offers here a number of specific recommendations.

3. Material Scope

18. The EDPS stresses that data transfers under the Framework Agreement may lead to serious legal and other consequences for the affected travellers, similar to those in the field of law enforcement and criminal justice, such as deprivation of liberty[19]. Furthermore, they affect a significant number of individuals. Consequently, the EDPS underlines that it is essential to ensure that the envisaged processing of personal data does not exceed the limits of what is strictly necessary and proportionate and, to this end, the scope of the Framework Agreement should be very clearly and narrowly defined.

19. The EDPS considers that the exchange of personal data under the Framework Agreement should be restricted to transfers of personal data of 'high-risk travellers', i.e. travellers for which there are objective indications that may pose a sufficiently serious risk, in line with the principles of proportionality and necessity.

20. The EDPS positively notes that the material scope of the Framework Agreement is limited to cases where the entry or stay of a given individual would pose a 'serious and genuine risk to public security or public order'[20]. The EDPS considers that this condition for the exchange of data, if implemented effectively and consistently, would serve as a key safeguard against possible systematic and indiscriminate checks of people traveling to the U.S. and to the EU, respectively.

21. At the same time, the EDPS notes that the concept of 'public order' is not a defined uniform concept of EU law, nor is it exhaustively defined by the terms of the Framework Agreement. As a result, it might encompass both criminal offences and administrative infringements, depending on domestic laws. Consequently, the inclusion of risks to 'public order' as a threshold for the request of personal data by a competent authority risk extending, in an unclear and unprecise manner, the material scope of the Framework Agreement.

[18] See Article 5 of the Annex to the Proposal, COM(2026) 484 final.
[19] EDPS Opinion 24/2025 on the negotiating mandate for a framework agreement between the European Union and the United States of America on the exchange of information for security screenings and identity verifications, issued on 17 September 2025.
[20] See Articles 6 and 7 of the Annex to the Proposal, COM(2026) 484 final.

22. The EDPS recalls that, in contrast to public order, public security constitutes one of the limited grounds for restricting data subject rights under Union data protection law. In the *Tsakouridis* judgment the CJEU clarified that 'a threat to the functioning of the institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or to peaceful coexistence of nations, or a risk to military interests, may affect public security'[21]. For instance, 'trafficking in narcotics as part of an organised group could reach a level of intensity that might directly threaten the calm and physical security of the population as a whole or a large part of it constituting a threat to public security'[22]. Accordingly, acts posing a risk to public security must be sufficiently serious to threaten the integrity of the state or its population.

23. The EDPS recommends that the bilateral agreements should further specify the types of offences that could be considered as risks to public order and public security or other objective criteria determining which acts and crimes could pose such risks (e.g. by establishing clear thresholds with reference to possible prison sentences). In the same vein, the Joint Committee to be established pursuant to Article 27 of the Framework Agreement, could be tasked to provide further interpretative guidance on the concept of 'public order', in line with Article 27(3) of the Annex, and to monitor how this aspect is applied in practice.

24. In addition, the EDPS recommends the Member States to carefully designate, in their bilateral agreements, the relevant national information systems from which information may be exchanged[23]. Only information systems relevant in the context of border and immigration control that contain information that is directly relevant, adequate and necessary for the assessment of whether there is a serious and genuine risk to public security or public order, should be designated. For instance, terrorists' watchlists or databases containing information about convicted persons and suspects of serious crimes such as drug trafficking, migrant smuggling or human trafficking, etc. This would ensure that the requirements for the exchange of personal data, which relate to the severity of risk to public order or public security, are satisfied by limiting the queries and the subsequent exchange of information to offences that meet the requisite level of seriousness to justify the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter.

4. Individuals concerned

25. The EDPS considers that the scope of the individuals concerned by of the envisaged exchange of personal data between the competent authorities of the Member States and of the U.S. is one of the key elements for the assessment of its proportionality. The proposed Framework Agreement would impact individuals crossing the U.S. borders or the borders of the concerned EU Member States or applying for a travel authorisation or a visa to enter or stay in the territory of one of the Member States of the EU or of the U.S. (hereinafter, "travellers")[24]. The Framework Agreement envisages processing of personal data of U.S. nationals, EU citizens and third country nationals.

[21] Judgment of the Court of Justice of 23 November 2010, *Land Baden-Württemberg v Panagiotis Tsakouridis*, C-145/09 ECLI:EU:C:2010:708, paragraph 44.
[22] Ibid., paragraphs 45-47.
[23] See Article 5 (b) of the Annex to the Proposal, COM(2026) 484 final.
[24] See Article 1.1 of the Annex to the Proposal, COM(2026) 484 final.

26. The EDPS notes that, in accordance with Article 7(3) of the Framework Agreement, the transfer of personal data is restricted to travellers with a 'nexus' to EU Member States or the U.S., including through citizenship or nationality; current or former residency or by having previously visited or stayed on their territory. The EDPS considers that while in the case of citizenship or (long-term) residence, the link of the traveller to the EU Member State or the U.S. is clear, the criteria of third country nationals visiting or just applying for visa should be further specified. In view of the principle of proportionality, the nexus should be better defined and should be concrete and verifiable (e.g. the nexus could be usefully specified in relation to objective criteria such as the duration of the stay or the relatively recent nature of the visit).

27. In light of the above, the EDPS recommends further specifying in the bilateral agreements the notion and the criteria to be fulfilled for a 'nexus' to a given country to exist, in particular of third country nationals. In this regard, the EDPS considers that brief occasional entries and stays, especially if they have taken place years ago, should not, in principle, be considered as establishing such a nexus. In the same spirit, the Joint Committee to be established pursuant to Article 27 of the Framework Agreement, could be tasked to provide further interpretative guidance also on the concept of 'nexus' and to monitor how it is applied in practice.

5. Criteria for determining the existence of risk

28. The EDPS notes that Part 2 of the Framework Agreement contains provisions setting the necessary conditions for the exchange of information, including the rules governing the automated exchange of limited personal data necessary for the identification of individuals during the assessment of an application for a travel authorisation or visa, or during a border check. Article 7 provides that, where, in the course of such an assessment, there is *'reason to believe'* that the entry or stay of an individual could pose a serious and genuine risk to public security or public order, a query can be submitted in relation to this individual.

29. Article 7(1) of the Framework Agreement refers to a 'reason to believe that the entry or stay could pose a serious and genuine risks (...)', without expressly specifying the nature of such ground. At the same time, the provision includes a non-exhaustive list of examples that might constitute criteria for determining the existence of such risk:

    i. where there are indications of identity fraud or misuse of identities;

    ii. where there are doubts as to the authenticity and validity of the travel documents;

    iii. where there are indications that an application for a visa contains fraudulent or false information;

    iv. where there are risk assessments and scenarios identifying risk on the basis of trend analysis of suspicious activity, law enforcement cases, or criminal intelligence; or

    v. where information about the concerned individual exists in the national information systems.

30. The EDPS considers that the criteria set in (i), (ii) and (iii) could reasonably trigger, at least, the first step under Article 7 of the Framework Agreement - the exchange of information

through an automated query for the purpose of verifying the identity of the individual. Regarding the (iv) criterion, the EDPS considers 'law enforcement cases' should be understood as criminal investigations, convictions, arrests or detentions involving the individual as a suspect or convicted person. This aspect, together with criminal intelligence, appear reasonable to determine the existence of potential risks, subject to case-by-case assessments.

31. At the same time, the 'risk assessments and scenarios identifying risk on the basis of trend analysis of suspicious activity' criterion raises concerns about the risk of profiling of travellers where patterns are used to formulate predictions of possible administrative infringements, criminal offences, or immigration violations, rather than assessing objective and verifiable facts. Profiling raises serious technical, legal and ethical questions. In particular, profiling is indispensably related to a high degree of generalisation and uncertainty regarding the accuracy of attributing certain patterns to particular features of individuals, which may result in the unjust treatment of certain groups of people[25].

32. In the *Ligue des droits humains* judgment, the Court of Justice of the European Union (CJEU) interpreted the terms 'sufficient grounds' and 'reasonably' in the PNR Directive as requiring 'objective material capable of giving rise to a reasonable suspicion that the person concerned is involved in one way or another in serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air, whereas, as regards terrorist offences having such a link, that requirement is satisfied when there is objective material from which it can be inferred that the PNR data could, in a given case, contribute effectively to combating such offences'[26]. Given the similar purpose of the PNR Directive and the Proposal, it is apparent that, following the CJEU's interpretation, there must be an objective link between the individual and the serious and genuine risk from which it can be inferred that the exchange of personal data could, in a given case, contribute effectively to preventing or combating risks to public security and public order.

33. Consequently, the EDPS considers that the criteria used to determine whether there are reasons to believe that the individual pose a serious and genuine risks for public security or public order should be fully in line with the fundamental rights enshrined in the Charter, particularly with the rights to privacy, data protection and non-discrimination. For that purpose, the EDPS considers that the agreement needs to be interpreted in such a way that trend analysis of suspicious activity should not be used as the *sole* basis for the identification of risks. Instead, risk assessment based on general trend analysis should be further substantiated by objective criteria in each specific individual case.

34. Regarding the criterion (v), it appears to suggest that whenever information about the concerned individual exists in the national information systems, competent authorities can rely on a justified suspicion on the existence of a risk. The EDPS warns against interpreting this criterion in such a general and broad manner, which does not distinguish between the different types of national information systems, nor the different categories of data subjects such as victims, witnesses, convicted persons or suspects, among others. In this regard, the EDPS underlines that the mere existence of personal data of the traveller concerned in any database cannot automatically be considered as objective material.

[25] See Fundamental Rights Agency (FRA), Preventing unlawful profiling today and in the future: a guide, issued on 5 December 2018.
[26] Judgment of the Court of Justice of 21 June 2022, *Ligue des droits humains*, C-817/19, ECLI:EU:C:2022:491, paragraphs 219, 220.

35. Therefore, the EDPS stresses the need for a careful case-by-case assessment whether the reason to believe that the entry or stay of an individual could pose a serious and genuine risk to public security or public order is based on objective elements that establish an objective link between the risk to public security or public order and the individual concerned. Only when the 'reason to believe' is objectively substantiated, the Requesting Competent Authority should be able to submit an automated query.

6. Justification of the query

36. In accordance with Article 7(7) of the Framework Agreement, when an automated query results in a match with information held in the Requested Competent Authority's national information systems, it should transfer to the Requesting Competent Authority through automated process confirmation of the match and alphanumeric data for the identification of the individual. The Requested Competent Authority should also assess without delay whether the match relates to a risk falling within Article 6, namely, a serious and genuine risk to public security or public order. This assessment is to be based on all relevant factors capable of establishing the existence of a risk, with the Framework Agreement identifying in Article 8 a non-exhaustive list of such indicators (criminal convictions, terrorist threats or immigration violations).

37. The EDPS positively notes that pursuant to Article 19 of the Framework Agreement, the Competent Authorities should have in place effective methods of demonstrating the lawfulness of processing of personal information, which may include the use of logs containing a 'clear and specific purpose of each query'. In the same vein, in case of a positive match under Article 7 and after the procedures described in Article 8 have been completed, the Requested Competent Authority may request from the Requesting Competent Authority 'contextual data' on the individual exclusively for ensuring accuracy and for auditing existing records on the individual concerned[27].

38. At the same time, to the EDPS notes that there is no explicit requirement for the Requesting Competent Authority, at the stage of the automated query process pursuant to Article 7, to indicate to the Requested Competent Authority the reason that gave rise to the belief that the individual may pose a risk; or whether the potential risk concerns public security or public order.

39. The EDPS understands that requiring the Requesting Competent Authority to disclose the specific reasons giving rise to the belief that an individual may pose a risk could, in certain cases, involve the disclosure of sensitive information, including information relating to national security, and that there may therefore be legitimate reasons for not systematically requiring such information to be communicated. At the same time, the EDPS considers that this does not necessarily preclude the provision of, at least, information concerning the nature of the risk, such as an indication of whether it relates to public security or public order. Without sufficient information, it may be difficult for the Requested Competent Authority to conduct a proper assessment of the match and to determine whether the

[27] See Article 9(6) of the Annex to the Proposal, COM(2026) 484 final.

processing of the personal data, and any further exchange of information, is necessary and proportionate in the circumstances of the individual case.

40. This is particularly relevant in light of Article 12(4) of the Framework Agreement, pursuant to which the Parties should ensure, under their respective legal frameworks, that personal data is processed in a manner that is directly relevant to, and not excessive or overbroad in relation to, the purpose of the processing. Providing the Requested Competent Authority with a clear indication of at least the nature of the risk underlying the query would facilitate the effective application of the principles of necessity and proportionality enshrined in this provision, by enabling the Requested Competent Authority to assess the match against the relevant benchmarks.

41. Against this background, the EDPS recommends that the technical procedure for encoding the query referred to in Article 7(5) should include a dedicated field allowing the Requesting Competent Authority to indicate at least the nature of the identified risk, for instance through a drop-down menu. Furthermore, when legitimate restrictions based, e.g. on national security, do not apply, the Requesting Competent Authority should in principle also indicate the specific reasons giving rise to the belief that an individual may pose a risk. This would provide the Requested Competent Authority with relevant contextual information while keeping the information exchanged limited to what is necessary for the assessment of the match.

7. Special categories of personal data

42. The exchange of information under the Framework Agreement may include a number of special categories of personal data: (1) fingerprints of the traveller as a component of the first step or automated query; and (2) additional information about a given individual in case of a match against a queried database, which may include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, additional genetic and biometric data, health data, or data concerning a natural person's sex life or sexual orientation[28]. The EDPS notes that the processing of special categories of personal data may increase the likelihood and severity of the interference with the rights and freedoms of natural persons.

43. In addition, for the confirmation of a risk, the requested competent authority might share personal data relating to criminal convictions and offences or related security measures. Due to the particular sensitivity of such data, the processing 'is liable to constitute a particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter'[29].

44. The EDPS notes that Article 20 of the Framework Agreement restricts the processing of special categories of personal data 'only under appropriate safeguards in accordance with

[28] See Articles 7 to 9 of the Annex to the Proposal, COM(2026) 484 final.

[29] Judgment of the Court of Justice of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraphs 74-75.

law'. The EDPS also positively notes that Article 7(2) lays down a prohibition to arbitrarily and unjustifiably discriminate against individuals on the grounds of sensitive personal data.

45. Lastly, the EDPS notes that Article 9(3) of the Framework Agreements limits the transfers of special categories of personal data, with the exception of biometric data for the purpose of uniquely identifying a natural person, only to cases where it is 'particularly relevant'. In this regard, the EDPS considers that, in order to comply with the Charter, the notion of 'particularly relevant' should be interpreted and applied in conformity with the condition of 'strict necessity' in the EU data protection legal framework[30].

8. Purpose limitation and further processing

46. Article 12 of the Framework Agreement sets out the purpose limitation for the processing of personal data within its scope. In particular, it provides that personal data may not be further processed in a manner that is incompatible with the purposes for which they were originally transferred. Paragraph 3 identifies specific purposes that are considered compatible with the original purpose (i.e. (i) purposes relating to the prevention of an immediate and serious threat to public security, (ii) reporting to public oversight authorities such as those listed in Article 26, and (iii) purposes directly related to those for which the information was exchanged under the Framework Agreement).

47. Paragraph 5 complements these provisions by requiring the Parties to ensure, under their respective legal frameworks, that personal data is processed in a manner that is directly relevant to, and not excessive or overbroad in relation to, the purpose of the processing. In addition, pursuant to paragraph 4, the Requested Competent Authority may require the Requesting Competent Authority to provide information concerning the use made of the transferred information.

48. The EDPS recalls that purpose limitation is a fundamental data protection principle which contributes to transparency, legal certainty and predictability, while protecting data subjects against the use of their personal data for purposes that they could not reasonably foresee. In the context of international data transfers, this principle is particularly relevant, since the transfer of personal data to another authority may otherwise result in a significant loss of control over the subsequent processing of those data especially in the context of onward sharing[31] and onward transfers[32].

49. While welcoming the prohibition on further processing for incompatible purposes as well the identification of certain compatible purposes and the safeguards set out in paragraph 4, the EDPS notes that the third and more general category[33] of compatible purposes in paragraph 3 is formulated in very general terms. As a result, it may give rise to questions

[30] See e.g. Article 10 of Directive (EU) 2016/680 (Law Enforcement Directive).
[31] The term onward sharing covers any subsequent sharing of personal data by a competent authority receiving the data from the competent data protection authority with a third party in its country. See EDPB Toolbox on essential data protection safeguards for enforcement cooperation between EEA data protection authorities and competent data protection authorities of third countries issued 14 March 2022.
[32] The term onward transfer covers any transfer of personal data by a receiving competent authority to a third party in another country. See EDPB Toolbox on essential data protection safeguards for enforcement cooperation between EEA data protection authorities and competent data protection authorities of third countries issued 14 March 2022.
[33] I.e. 'purposes directly related to those for which the information was exchanged under the Framework Agreement'.

as to the foreseeability of certain forms of further processing in relation to the original purpose. This consideration is particularly relevant when the provision is read in conjunction with Article 13(1), which also refers to law enforcement, regulatory or administrative authorities and may therefore potentially broaden the range of circumstances in which the transferred data could subsequently be processed.

50. Against this background, the EDPS considers that particular importance should be given to the qualifier 'directly' in assessing whether a further processing activity falls within the third category of compatible purposes. The direct link to the original purpose should be assessed in light of specific factors, such as the relationship between the original and intended purposes, the nature of the personal data, the potential consequences for data subjects, the existence of appropriate safeguards, etc.. In this way, the qualifier 'directly' would represent an important limitation on the scope of the further processing.

51. Furthermore, the EDPS emphasizes that the effectiveness of this limitation in ensuring the foreseeability and compatibility of further processing will depend on how this requirement is applied in practice and, in particular, on whether the relevant factors are duly taken into account when determining whether a sufficiently close link with the original purpose exists. Therefore, the EDPS recommends that the Joint Committee should review the practical implementation of the 'directly related' criterion, in conjunction with Article 13(1) of the Framework Agreement, to ensure that it is relied upon as a broad or open-ended basis for further processing.

9. Onward sharing and transfers

52. The EDPS considers that, where onward sharing is necessary, it should generally be permitted only where the transferring public body has given its prior authorisation and the receiving third party commits to respect the same data protection principles and safeguards as those provided for in the international agreement[34].

53. The current text of the Framework Agreement allows for onward sharing of transferred personal data without requiring the prior authorisation of the Requested Competent Authority[35]. At the same time, the EDPS positively notes that Article 13(1) requires the third party receiving the data to comply with the applicable data protection principles and safeguards provided for in Part 3 of the Framework Agreement, which include the purpose limitation set out in Article 12. While this provides an important safeguard for the protection of the data following onward sharing, the absence of a prior authorisation requirement, combined with the absence of a mandatory notification to the Requested Competent Authority, may limit the ability of the Requested Competent Authority to retain a meaningful overview of the subsequent use and sharing of the personal data it has transferred. This consideration is further relevant in light of the fact that, as noted above, the third category of compatible purposes under Article 12(3) is formulated in general terms.

[34] See also EDPB Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, V0.2 Adopted on 15 December 2020, available here.
[35] See Article 13 of the Annex to the Proposal, COM(2026) 484 final.

54. The EDPS recognises that it may be difficult in practice to exhaustively specify the circumstances in which onward sharing may be necessary, as the need for such sharing may arise from circumstances that cannot reasonably be anticipated at the time of the initial transfer. Nevertheless, where prior authorisation is not required, the EDPS considers that an appropriate notification requirement would provide an important additional safeguard and help balance the need for operational flexibility with the need to ensure meaningful control over subsequent use and sharing.

55. In this context, the EDPS notes the possibility under Article 12(4) for the Requested Competent Authority to require the Requesting Competent Authority to provide information concerning the use made of the transferred information. This mechanism may help preserve meaningful purpose limitation and ensure that the transferring authority, and ultimately data subjects, retain a degree of control over the subsequent use of the data. Its effectiveness, however, would be enhanced if the Requested Competent Authority were systematically informed of onward sharing, rather than having to rely on information provided subsequently upon request. Therefore, the EDPS invites Member States to consider ensuring, in their bilateral agreements, that the Requested Competent Authority is informed of onward sharing in an appropriate and effective manner.

56. As regards onward transfers, the EDPS welcomes that Article 14 of Framework Agreement requires the prior consent of the Requested Authority, which is required to carry out an assessment before granting such consent. It also understands that a negative outcome of this assessment should preclude the granting of consent to the onward transfer.

10. Judicial and administrative redress

57. The EDPS notes that Article 24 of the Framework Agreement lays down the obligation of the Parties to provide administrative and judicial redress for individuals, whose personal data has been processed and used in a manner inconsistent with the provisions on the protection of personal data of the Framework Agreement.

58. The EDPS considers the general reference to 'individuals' as foreseeing the availability of administrative and judicial remedies to anyone regardless of their nationality or citizenship. The EDPS also recalls that, according to the CJEU, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to them, or to obtain the rectification or erasure of such data, would not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter of Fundamental Rights[36].

59. The EDPS therefore reiterates its previous recommendation about the need to ensure in practice that judicial redress will be available for all data subjects, irrespective of their citizenship, and calls on the Commission to monitor closely this element[37].

[36] Judgment of the Court of Justice of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 95 (Schrems I)
[37] EDPS Opinion 24/2025 on the negotiating mandate for a framework agreement between the European Union and the United States of America on the exchange of information for security screenings and identity verifications, issued on 17 September 2025.

11. Effective oversight

60. The EDPS recalls that Article 8(3) of the Charter provides that respect for the rules on data protection has to be supervised by an independent authority[38], which means, according to the CJEU, an authority able to make decisions independently from any direct or indirect external influence. Such a supervisory authority must not only be independent from the parties it supervises, but must also not be part of the government, since the government itself may be an interested party. In this context, the EDPS positively notes the requirement under Article 26(1)(a) that oversight authorities must 'exercise independent oversight functions and powers'.

61. At the same time, the EDPS considers it essential that the competent oversight authorities, as well as the powers they may exercise, are clearly identified and known to the Parties before any transfer takes place. In this regard, the EDPS notes that, while Article 26(2) of the Framework Agreement clearly defines the oversight bodies on the EU side, i.e. the data protection authorities of its Member States, paragraph 3 does not provide similar clarity as regards the oversight on the U.S. side.

62. Therefore, the EDPS recommends that before the start of the provisional application of the Framework Agreement, the U.S. must formally notify to the EU its supervisory authorities that have competence in this matter, including their specific tasks and powers. In addition, the EDPS considers that there should be a mechanism for the Parties to inform each other about future changes in oversight bodies.

63. The EDPS also recalls that the privacy notice to be provided to data subjects, pursuant to Article 25 of the Framework Agreement, should include the contact details or, at a minimum, the name of the oversight authority before which they may exercise their rights.

12. Suspension and termination

64. Article 29(1) of the Framework Agreement allows both Parties to suspend the Framework Agreement in whole or in part in the event of a 'material breach', after a reasonable period of consultation. In this regard, the EDPS positively notes that this provision permits the suspension of the Framework Agreement, in cases of violations of the essential elements of it, such as Part 3 on the protection of personal data. To this effect, the EDPS stresses the paramount role of independent oversight of the application of the Framework Agreement in order for breaches to be identified.

65. In its Opinion 24/2025 on the negotiating mandate, the EDPS welcomed that the negotiating directives envisaged an explicit provision in the framework agreement whereby a Party may terminate or suspend it, 'in particular where the U.S. no longer effectively ensures the level of protection of fundamental rights and freedoms required

[38] *Schrems I*, paragraphs 57 and 65.

under the framework agreement'[39]. The EDPS notes that a similar wording is absent in the Framework Agreement.

66. The EDPS nevertheless considers, also in the light of the international human rights legal instruments referred in the preamble of the Framework Agreement, to which both the EU Member States and the U.S. are Parties, that grave violations of fundamental rights and freedoms in the context of the Framework Agreement, such as arbitrary detentions or inhuman or degrading treatments, by any of the Parties, can and should be interpreted as constituting a material breach.

67. In addition, Article 11 of Framework Agreement lays down the possibility of the Requested Competent Authority, by virtue of the respective bilateral agreement, to refuse a request of personal data 'if it would conflict with international obligations'. The EDPS underlines that such international obligations include, among others, also the human rights treaties mentioned in the preamble, such as the Convention against Torture and Other Cruel, Inhuman and Degrading Treatment or Punishment.

68. However, the EDPS notes that, in practice, it may be difficult for the Requested Competent Authorities to carry out such a complex assessment on the compliance of the Requesting Competent Authorities with human rights obligations. Therefore, the EDPS calls on the Commission to monitor closely and regularly assess the situation.

13. Conclusions

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

(1) the bilateral agreements should designate only national information systems that contain information that is directly relevant, adequate and necessary for the assessment of whether there is a serious and genuine risk to public security or public order;

(2) the bilateral agreements should further specify the types of offences that could be considered as risks to public order and public security, or lay down other objective criteria (e.g. by establishing clear thresholds with reference to possible prison sentences).

(3) the bilateral agreements should further specify the notion and the criteria to be fulfilled for a 'nexus' to a given country to exist.

(4) the Competent Authorities should carry out careful case-by-case assessment whether the reason to believe that the entry or stay of an individual could pose a serious and genuine risk to public security or public order is based on objective elements that establish an objective link between the risk to public security or public order and the individual concerned.

(5) the Requesting Competent Authority should, as a rule, indicate the specific reasons giving rise to the belief that an individual may pose a risk. In the same vein, the technical procedure

[39] EDPS Opinion 24/2025 on the negotiating mandate for a framework agreement between the European Union and the United States of America on the exchange of information for security screenings and identity verifications, issued on 17 September 2025, p. 16, 17.

for encoding the query referred to in Article 7(5) should include a dedicated field allowing the Requesting Competent Authority to indicate, at least, the nature of the identified risk.

(6) the notion of 'particularly relevant' in the context of the processing of special categories of personal data should be interpreted and applied in accordance with the condition of 'strict necessity' in the EU data protection legal framework.

(7) the Joint Committee should regularly review the practical implementation of the 'directly related' criterion in the context of further processing.

(8) the bilateral agreements should ensure that the Requested Competent Authority is informed of the onward sharing in an appropriate and effective manner.

(9) the Commission should closely monitor whether judicial redress is available in practice for all data subjects, irrespective of their citizenship or nationality.

(10) before the start of the provisional application of the Framework Agreement, the U.S. side should formally notify to the EU about its competent supervisory authorities, including their specific tasks and powers.

(11) a mechanism should be put in place for the Parties to inform each other about future changes in their oversight authorities.

(12) the Commission should monitor closely and regularly assess the compliance with human rights obligations as a ground for possible suspension or termination of the Framework Agreement.

Brussels, 27 October 2026

(e-signed)
Wojciech Rafał WIEWIÓROWSKI