



EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data
protection authority

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

The European Data Protection Supervisor (EDPS) is an independent institution of the European Union (EU), responsible under Article 52(2) of Regulation (EU) 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) of Regulation (EU) 2018/1725 ‘... 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 (EU) 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 Recommendation for a Council Decision authorising the opening of negotiations on a framework agreement between the European Union and the United States of America on the exchange of information for security screenings and identity verifications relating to border procedures and applications for visa¹.

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 Recommendation that are relevant from a data protection perspective.

¹ COM(2025) 447 final.

Executive Summary

On 23 July 2025, the European Commission issued a Recommendation for a Council Decision authorising the opening of negotiations on a framework agreement between the European Union and the United States of America on the exchange of information for security screenings and identity verifications relating to border procedures and applications for visa.

The objective of the proposed Recommendation is to provide the negotiating directives to the European Commission to negotiate a framework agreement that will set out the legal structure and conditions for the exchange of information between the competent authorities of the EU Member States and of the United States, based on which the Member States would be empowered to establish bilateral agreements for an exchange of information from their national systems. The Recommendation is linked to the requirement by the United States for admission to and further participation in the U.S. Visa Waiver Program, pursuant to which the partner countries have to conclude of an 'Enhanced Border Security Partnership' (EBSP) with the U.S. Department of Homeland Security.

The EDPS notes that the proposed framework agreement, if concluded, 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 by a third country. Therefore, the EDPS stresses the need to ensure that the envisaged processing of personal data does not exceed the limits of what is strictly necessary and proportionate. In the light of this, he largely supports the proposed approach to establish a common EU-U.S. framework for such information exchange that would set common Union-level conditions and safeguards and thus, in his view, contribute to more effective guarantees and subsequently stronger protection of the fundamental rights and freedoms of the affected individuals. To this end, the EDPS urges the Commission and the Council to take into account a number of specific recommendations.

The EDPS considers it necessary to conduct an in-depth fundamental rights impact assessment of the proposed framework agreement and the Enhanced Border Security Partnerships with the United States. In that context, he believes that the seriousness of the interference by the proposed sharing of personal data for the purposes of border and immigration control by the United States should be deemed comparable to the seriousness of the interference caused by the exchanges of data for law enforcement purposes.

Additionally, the EDPS recommends to define the personal scope of the framework agreement exhaustively and narrowly, taking also into account the specific prohibitions of data sharing laid down in EU law. In the same vein, he recommends that the categories of personal data that may be exchanged under the framework agreement, including the content and the scope of the supplementary information to be provided to the U.S. authorities, should also be circumscribed exhaustively and as narrowly as possible. Moreover, the EDPS explicitly underlines that any direct or indirect sharing and transfer of data from the EU large-scale IT systems in the area of justice and home affairs and in particular from those related to migration and asylum, should be precluded.

The EDPS makes also other important recommendations, including about the accountability mechanisms, in particular the need for clear and specific justification of each query; the transparency of the envisaged processing and the corresponding obligations of the competent U.S. and EU authorities; the legal possibility for EU Member States to refuse sharing or transferring data to U.S. authorities in individual cases; the availability of judicial redress in the United States regardless of the citizenship and the purposes of the processing; and others.

Contents

1. Introduction.....	5
2. General remarks	6
3. Legal basis and applicable legal framework on data protection.....	7
4. Necessity and proportionality	8
4.1. Material scope	9
4.2. Personal scope	10
4.3. Categories of personal data.....	11
4.4. Modalities for exchange of personal data	13
4.5. Data protection safeguards	14
4.6. Transparency	15
4.7. Oversight and redress	16
5. Suspension and termination	16
6. Conclusions	17

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union (TFEU),

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 23 July 2025, the European Commission issued a Recommendation for a Council Decision authorising the opening of negotiations on a framework agreement between the European Union and the United States of America on the exchange of information for security screenings and identity verifications relating to border procedures and applications for visa³ ('the Recommendation').
2. The objective of the proposed Recommendation is to provide the negotiating directives to the European Commission to negotiate a framework agreement that will set out the legal structure and conditions for the exchange of information between the competent authorities of the EU Member States and of the United States, based on which the Member States would be empowered to establish bilateral agreements for an exchange of information with the United States from their national information systems⁴.
3. The Recommendation is linked to the new requirement by the United States of America 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. The new requirement entails the conclusion of an 'Enhanced Border Security Partnership' (EBSP) with the U.S. Department of Homeland Security (DHS)⁵. 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. VWP⁶.
4. The present Opinion of the EDPS is issued in response to a consultation by the European Commission of 23 July 2025, pursuant to Article 42(1) of EUDPR. The EDPS welcomes the reference to this consultation in Recital 3 of the Recommendation. In addition, given the expected significant impact on the proposed agreement on the rights to privacy and protection of personal data, the EDPS stands ready to provide further advice to the Commission as Union negotiator in the course of the negotiations.

² OJ L 295, 21.11.2018, p. 39.

³ COM(2025) 447 final.

⁴ See See Explanatory Memorandum, COM(2025) 447 final, p.1.

⁵ See Recital 1 of the Recommendation, COM(2025) 447 final, p.6.

⁶ See Explanatory Memorandum, COM(2025) 447 final, p.1.

2. General remarks

5. The conclusion of an Enhanced Border Security Partnership 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 requirements such as the Agreements on Enhancing Cooperation in Preventing and Combating Serious Crime (PCSC Agreements), which establish information exchange, including biometric data, on individuals who are suspected or convicted of terrorist offences or serious crime⁷.
6. The United States has set a deadline 31 December 2026 for the conclusion of the EBSP agreements with the countries admitted to the VWP, including the EU Member States⁸. It should be noted that the proposed framework agreement differs from the existing EU agreements with third countries, including with the United States, that entail large-scale transfers of data, such as the Passenger Name Record (PNR) agreements or the EU-U.S. TFTP Agreement⁹. The material scope of these agreements is limited to law enforcement and criminal justice cooperation, and in some cases their scope is further restricted to combating only serious crime and terrorism.
7. The proposed framework agreement, if concluded, would therefore 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 by a third country.
8. Given the novelty of the subject matter and the expected significant impact on the fundamental rights of a large number of individuals, the EDPS notes with regret that the Recommendation is not accompanied by an Impact Assessment, which in this case would have been fully justified and would have facilitated the assessment of its necessity and proportionality.
9. This notwithstanding, the EDPS largely supports the proposed approach to establish a common EU-U.S. framework for information exchange in the context of the EBSP that would set common Union-level conditions and safeguards. Such an approach might, in his view, contribute to more effective safeguards and subsequently stronger protection of the fundamental rights and freedoms of the affected individuals.
10. This Opinion examines the necessity and proportionality of the proposed framework agreement as it would result if the negotiating directives were all fully implemented, focusing specifically on its purpose, material and personal scope and envisaged data protection safeguards, including oversight and redress mechanisms, and offers a number of concrete recommendations.

⁷ See Explanatory Memorandum, COM(2025) 447 final, p.1.

⁸ *Ibid.*

⁹ Agreement between the United States of America and the European Union on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010, pp. 5–14.

3. Legal basis and applicable legal framework on data protection

11. The EDPS notes that the legal basis of the Recommendation are the following provisions of the TFEU: Article 16(2), Article 77(2) and Article 218(3) and (4). Article 218 TFEU lays down the procedure for the negotiation and conclusion of agreements between the European Union and third countries or international organisations. Article 77(2) TFEU regulates matters related to, among others, the common visa policy and the checks of persons crossing external borders of the Union.
12. Under Article 16(2) TFEU, the Union has the power to adopt measures relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and by Member States when carrying out activities which fall within the scope of Union law.
13. In line with the jurisprudence of the CJEU, Article 16 TFEU provides an appropriate legal basis in cases where the protection of personal data is one of the essential aims or components of the rules adopted by the EU legislature¹⁰.
14. The EDPS considers that it can indeed already be considered that the protection of personal data is (and should be) one of the essential aims and components of the future framework agreement and therefore supports the inclusion of Article 16 TFEU among substantive legal bases of the Recommendation.
15. The other interlinked aims of the agreement are to further law enforcement cooperation and immigration control. In that context, one of the consequences of the interlinked law enforcement and immigration objectives of the EBSP is the potential applicability of different data protection regimes under the EU data protection legal framework. The processing of data by criminal law enforcement authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties is covered by Directive (EU) 2016/680 ('the LED')¹¹, while processing of personal data by Member States for purposes like immigration control and visa policy is governed by Regulation (EU) 2016/679 (the 'GDPR'). Both the GDPR and the LED include strict conditions for the transfer of personal data to third countries.
16. In addition, for data transfers between criminal law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offenses, including terrorism, the EU and the United States have signed in 2016 the so-called 'Umbrella Agreement', which is intended to provide appropriate safeguards within the meaning of Article 37(1)(a) of the LED¹². The Umbrella Agreement supplements, as appropriate, but does not replace, provisions regarding the protection of personal data in the existing and future law

¹⁰ See Opinions of the Court of Justice of 6 October 2021, A-1/19 par. 284-285 and of 26 July 2017, *PNR Canada*, ECLI:EU:C:2017:592, par. 96. See also [EDPB- EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence \(Artificial Intelligence Act\)](#), issued on 18 June 2021, par. 11.

¹¹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.

¹² 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 ('Umbrella Agreement'), OJ L 336, 10.12.2016.

enforcement agreements between the EU Member States and the United States. At the same time, the Umbrella Agreement on its own is not construed to provide the legal basis for any transfers of personal data¹³.

17. As acknowledged by the Commission in the Explanatory Memorandum¹⁴, given the broader scope and purpose of the information exchange intended by the EBSF, and to the extent that authorities other than criminal law enforcement would be involved in the transfer, the EU-U.S. Umbrella Agreement is not entirely applicable to all the types of transfers envisaged by the United States under the EBSF.
18. Consequently, one of the objectives of the framework agreement is to fill this gap and to lay down the safeguards and guarantees needed with regard to the protection of personal data as well as fundamental rights and freedoms of individuals affected by the exchange of personal data in the context of the EBSF¹⁵.
19. The EDPS is concerned that the distinction in practice between the applicable legal acts on data protection, i.e. the GDPR and the LED, might prove challenging, especially in view of possible divergent understanding in the EU and in the United States of the concepts of security and law enforcement. Therefore, the EDPS urges the Commission to circumscribe very clearly in the framework agreement the purposes and the objectives of the envisaged data processing operations under the EBSF, in order to ensure the necessary legal clarity and certainty regarding the applicable legal framework on data protection in the EU, especially if the transfer of personal data for non-law enforcement purposes in the U.S. is retained in the agreement.

4. Necessity and proportionality

20. Article 52(1) of the Charter of Fundamental Rights ('the Charter') allows limitations to be placed on the exercise of the rights to privacy and protection of personal data enshrined Articles 7 and 8 of the Charter, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others¹⁶. In this context, an integral part of the proportionality test is the assessment of the seriousness of the interference by the envisaged processing of personal data.
21. The Court of Justice of the European Union (CJEU) has advanced several criteria to determine the seriousness of an interference with the right to the protection of personal data and the right for respect of private life, such as the objectives and purposes of the processing, the nature of the personal data, the categories and the number of affected data subjects, the nature and specific methods for the processing of the data at issue, etc. In that regard, the CJEU has repeatedly upheld the general principle that only significant and important objectives of public interest are capable of justifying a serious interference with

¹³ See Article 1(3) and Article 5(1) of the Umbrella Agreement.

¹⁴ See Explanatory Memorandum, COM(2025) 447 final, p. 4.

¹⁵ See point 11 of the Annex, COM(2025) 447 final.

¹⁶ See e.g. CJEU judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 120 and 121.

the fundamental rights¹⁷. Moreover, the greater the interference entailed by the proposed act is, the most robust and detailed the respective conditions and the safeguards should be.

22. In line with the above-mentioned principles and case law, the EDPS considers 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. To this end, the material and personal scope should be very clearly and narrowly defined. In particular, any potential exchange of personal data in the framework of the EBSPs should be limited only to people travelling to the United States. Moreover, as already envisaged in point 3 of the Annex to the Recommendation, the agreement should preclude a systematic, generalised and non-targeted processing of data for all travellers.

4.1. Material scope

23. According to the Recommendation, the purposes of the envisaged transfer and subsequent processing of personal data in the context of the EBSP are (1) ‘screening and verification of identity of travellers necessary to determine if their entry or stay would pose any risk to public security or public order’, and (2) ‘to support the competent authorities in the prevention, detection, investigation and prosecution of crimes and terrorist offences’¹⁸.
24. The EDPS notes the U.S. Department of Homeland Security (DHS) has published in 2024 a “Privacy Impact Assessment Update - DHS International Biometric Information Sharing (IBIS) Program – Enhanced Border Security Partnership (EBSP)”¹⁹, which explains in more details the purposes of the bilateral biometric and biographic information sharing between the United States and its foreign partners under the EBSP/IBIS Program, i.e. ‘border security, immigration decision-making, law enforcement activities with a nexus to the U.S. border, countering transnational crimes and organizations, detecting terrorism, and preventing and detecting crimes considered felonies under U.S. law or which render an individual inadmissible under the Immigration and Nationality Act’.
25. Transfers of personal data for the purpose of prevention, detection, investigation and prosecution of crimes and terrorist offences, while liable to have a significant impact on the lives of the individuals concerned, are also capable in principle to justify a more serious interference with fundamental rights enshrined in Articles 7 and 8 of the Charter, as explained in the above-quoted case law of the CJEU. Moreover, such processing falls in the scope of the EU-U.S. Umbrella Agreement and the respective safeguards laid down in it.
26. At the same time, the purpose of ‘screening and verification of identity of travellers’ and in particular ‘immigration decision-making’ by a third country authorities raises questions about its proportionality, especially if it would be carried out in a large scale, thus affecting a significant number of individuals.
27. The EDPS acknowledges the significance of the measures related to border and migration management. The recently adopted Pact on Migration and Asylum as well as the newly

¹⁷ See CJEU judgment of 6 October 2020, Joined Cases La Quadrature du Net and Others, C-511/18 and C-512/18, EU:C:2020:791, paragraphs 95-98, judgment of 2 October 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, paragraphs 54, 57 and 60, (judgment of 2 March 2021, Prokuratuur (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraph 35.

¹⁸ See point 2 of the Annex, COM(2025) 447 final.

¹⁹ DHS Reference No. DHS/ALL/PIA-095(b), available at https://www.dhs.gov/sites/default/files/2024-04/24_0429_priv_pia-dhs-all-095b.pdf

developed large-scale EU IT systems like the European Travel Information and Authorisation System (ETIAS) and the Entry/Exit System (EES) show the political importance of these policies for the Union.

28. At the same time, as the EDPS has repeatedly stressed, most recently on the occasion of the issuance of the EDPS Opinion on the Proposal for a Regulation establishing a common system for the return of third-country nationals staying illegally in the EU, data protection – as fundamental right listed in the Charter – is one of the last lines of defence for vulnerable individuals, such as migrants and asylum seekers²⁰. This is very relevant in the case of the proposed exchanges of personal data with the United States, given the well-known and widely recognised fact that the U.S. government applies a particularly strict immigration policy. Thus, it should be borne in mind that the transfer of personal data for the purposes of ‘screening and verification of identity of travellers’ may actually lead to serious legal and other consequences for the affected individuals, similar to those in the field of law enforcement and criminal justice, such as deprivation of liberty.
29. The EDPS therefore urges the Commission to fully take into account in the negotiations the legal and policy implications of the material scope of the future agreement. Specifically, the seriousness of the interference provoked by the proposed sharing of personal data with a third country for the purposes of border and immigration control by that country should be considered for all effects as comparable to the interference caused by the exchanges of data for law enforcement purposes.

4.2. Personal scope

30. According to the Explanatory Memorandum to the Recommendation, under the EBSP, the United States intends to establish an information exchange on:
- travellers to the United States who may have a connection to the VWP partner country;
 - applicants for immigration benefits or humanitarian protection in the United States;
 - individuals encountered by DHS law enforcement in a border and immigration context in the United States.
31. The personal scope of the proposed exchange of personal data between the competent authorities of the Member States and of the United States is one of the key elements for the assessment of its proportionality. In that regard, the EDPS notes that the negotiating directives in the Recommendation make an important distinction between EU citizens, on the one hand, and third-country nationals, on the other hand²¹.
32. According to point 7 of the Annex of the Recommendation, personal data of third-country nationals would be transferred for both immigration purposes (‘in relation to the crossing of the external borders’) and for law enforcement purposes (‘in the context of the prevention, detection, investigation and prosecution of crimes and terrorist offences’).

²⁰ See the EDPS press release of 28 May 2025, available at https://www.edps.europa.eu/press-publications/press-news/press-releases/2025/migration-management-data-protection-one-last-lines-defence-vulnerable-individuals_en

²¹ See points 7 and 8 of the Annex, COM(2025) 447 final.

33. By contrast, in accordance with point 8 of the Annex of the Recommendation, personal data of [EU] citizens, their family members and of permanent residents may be exchanged only for law enforcement purposes, moreover if ‘strictly necessary and proportionate’.
34. In addition, subject to specific safeguards, the framework agreement would also allow the transfer of personal data on minors and on victims of criminal offences, witnesses or other persons who can provide information concerning criminal offences²².
35. The EDPS understands that the exact modalities of the proposed data exchanges would be defined in the course of the negotiations. Notwithstanding this, he considers that still at the level of the negotiating mandate there should be sufficient clarity about the categories of data subjects potentially affected by the processing.
36. In that regard, the EDPS considers that the negotiating directives should clarify the notion of ‘family members’ and should lay down the conditions and the context in which personal data of a family member may be queried and shared. The EDPS believes that such processing should in principle be possible only if the family member is actually crossing the borders of the United States, or is planning to do so (e.g. by filling for the Electronic System for Travel Authorization (ESTA) or requesting visa). In the same vein, there should be clarity about the notion of ‘permanent residents’. For instance, in the context of EU migration and asylum laws, the two categories that come closest to it are long-term residents and people with refugee status.
37. Another aspect of the proposed framework agreement that could be deemed problematic from point of view of EU law is the envisaged exchange of personal data of ‘applicants for humanitarian protection in the US’, which seems to refer to asylum seekers. The EDPS recalls that the Union acts dealing with asylum and migration explicitly prohibit sharing such data from relevant EU IT system with third countries (with few limited exceptions, e.g. for readmission)²³.
38. The EDPS therefore recommends that the personal scope of the framework agreement is defined exhaustively and as narrowly as possible, in accordance with the principles necessity and proportionality, taking fully into account the specific prohibitions of data sharing laid down in EU law.

4.3. Categories of personal data

39. The CJEU has identified the nature of the processed personal data, in special categories of data, as another important criterion for the assessment of the seriousness of an interference with the right to the protection of personal data²⁴.

²² See point 11(e) of the Annex, COM(2025) 447 final.

²³ See Article 49(4) of Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of ‘Eurodac’ for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1351 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council (‘Eurodac Regulation’) (OJ L, 2024/1358, 22.5.2024).

²⁴ See for instance Judgment of 24 September 2019, GC and Others, C-136/17, EU:C:2019:773, par. 44; judgment of 25 January 2018, Bevéndorlási és Állampolgársági Hivatal, C-473/16; EU:C:2018:36, par. 59-63; judgment of 22 June 2021, Latvijas Republikas Saeima, C-439/19, EU:C:2021:504, par. 74-75.

40. According to the Recommendation, the exchange of information under the framework agreement may include several categories of personal data: (1) ‘core’ data, i.e. the identity information included in the travel document, and the fingerprints of a traveller; (2) supplementary information about a given individual in case of a match against a queried database; as well as (3) special categories of personal data²⁵.
41. In addition, the EDPS would like to point out that, in his understanding, a ‘hit/no hit’ reply in case of automatic queries against a database may also be considered as personal data and should be treated as such.
42. The EDPS is concerned specifically by the lack of clarity in the negotiating directives, even in broad terms, about the content and scope of the supplementary information, which seem to be left to be circumscribed in the bilateral agreements or arrangements with the individual Member States.
43. In this regard, the EDPS notes that in the already mentioned “Privacy Impact Assessment Update - DHS International Biometric Information Sharing (IBIS) Program – Enhanced Border Security Partnership (EBSP)” the U.S. DHS provides an indication about what additional information the U.S. authorities would be expecting from their counterparts in case of a match of the queried data (e.g. fingerprints) against the respective database: ‘biographic information to DHS on the associated identity (e.g., name, date of birth, travel documents, nationality) as well as any known criminal convictions and arrests for serious crimes’²⁶, and an indication of the individual’s immigration status in that country’²⁷.
44. The EDPS recalls that he has already commented in his Opinion on the Proposal for a Regulation on automated data exchange for police cooperation (Prüm II)²⁸ on the risk associated with the sharing of data from national police records, where the information about the possible arrests are typically stored. In particular, the EDPS had highlighted that national police records might contain data that had not been reviewed by a judicial authority, e.g. criminal intelligence about a potential ‘suspect’ in a crime, which had not been further pursued and investigated for various reasons. The concerns of the EDPS in his 2022 Opinion about the reliability of the information in the police records are even more relevant in the case at hand.
45. The EDPS also notes that the proposed negotiating directives are not clear whether the supplementary information would be requested in all cases of a match, or only if the query is conducted in the context of the prevention, detection, investigation and prosecution of crimes and terrorist offences. However, the mentioned public document by the U.S. DHS implies that the additional information, including about prior arrests, would be generally required also in cases of queries for non-law enforcement (e.g. immigration) purposes.
46. Regarding special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning a person’s health and sex life or sexual orientation, according the proposed negotiating directives, their transfer should only be possible where ‘strictly necessary and

²⁵ See points 6 and 11(e) of the Annex, COM(2025) 447 final.

²⁶ Under U.S. law a felony is a crime for which the penalty is more than one year of imprisonment.

²⁷ DHS Reference No. DHS/ALL/PIA-095(b), page 2.

²⁸ Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation, paragraphs 42, 43, https://www.edps.europa.eu/system/files/2022-03/22-03-07_opinion-4-2022_prum_en.pdf

proportionate in individual cases for preventing or combating criminal and terrorist offences as referred to in the framework agreement, and subject to appropriate safeguards'. The EDPS welcomes this specification and insists on its importance for ensuring the necessity and proportionality of the overall approach, given the sensitive nature of such data.

47. The EDPS therefore recommends that, in line with the principles of necessity and proportionality and data minimisation, the categories of personal data to be exchanged under the framework agreement should be circumscribed in the framework agreement exhaustively and as narrowly as possible, especially regarding the possible supplementary information to be provided to the authorities of the other Party as a result of a query for non-law enforcement purposes.

4.4. Modalities for exchange of personal data

48. Another element of the proposed negotiating mandate that sets a precedent for the international agreements at Union level and thus deserves specific attention is the envisaged mechanism for exchange of personal data.
49. The EDPS notes that point 15 of the Annex to the Recommendation seems to imply automatic access to certain Member States databases: '[t]he framework agreement should provide for a layered query response model, which distinguishes between information retrieved automatically upon performing a query and additional information which could be shared with the requesting Party only upon the explicit authorisation of that Party'.
50. This understanding is further supported by the publicly available information from the U.S. DHS, which clarifies that pursuant to the bilateral Enhanced Border Security Partnerships with foreign partners, DHS may be authorized to conduct a search against the partner's relevant national databases. In the event of a match, consistent with the terms of the applicable bilateral information sharing arrangement, the partner will provide additional information²⁹, as explained in the previous section of this Opinion.
51. Thus it may be deemed that the proposed mechanism for queries under the framework agreement and the EBSPs would in practice approximate the United States with the situation of EU Member States and the Schengen Associated Countries as regards automatic access to data, for instance in the context of the Prüm system of automated data exchange for police cooperation³⁰.
52. The EDPS notes that, according to points 10 and 12 of the Annex to the Recommendation, the framework agreement should outline the general conditions, criteria, types of databases and categories of data that would fall in scope of the exchange of information between the competent authorities of the Member States and of the United States as part of bilateral arrangements. On the other hand, the designation and the set-up of the queried national

²⁹ DHS Reference No. DHS/ALL/PIA-095(b), page 2.

³⁰ For more information see Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation), OJ L, 2024/982, 5.4.2024.

databases, as well as the other legal technical requirements or limitations, would be laid down in the bilateral arrangements operationalising the information exchange³¹.

53. In this context, the EDPS recalls that relevant national databases and the large-scale information systems used by EU Member States in the field of justice and home affairs, such as the Schengen Information System, the Visa Information System or Eurodac, are very much interlinked and interoperable. In addition, the architecture of many of these IT systems include central components, managed by a Union body - the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). Moreover, the EU interoperability framework provides for storing and accessing data, including identity and biometric data, in common interoperability components, such the Common Identity Repository, the shared Biometric Matching Service and the European Search Portal³².
54. In the same vein, the EDPS recalls the explicit prohibitions under the EU law of sharing of personal data from Union databases and IT systems with third countries and international organisation. For instance, as already pointed out in this Opinion, Article 49 of Regulation (EU) 2024/1358 (Eurodac Regulation) prohibits Member States and EU agencies from sharing data about refugee and migration status of third-country national that is stored in Eurodac. Similarly, Article 18 of Regulation (EU) 2019/816 (ECRIS-TCN Regulation)³³ prohibits sharing of information about criminal convictions of third-country nationals and stateless persons stored in the European Criminal Records Information System. The EDPS consider these safeguards as important ones and the framework agreement, which would take precedence over the mentioned provisions, should not overrule them.
55. The EDPS therefore stresses that the proposed framework agreement and the bilateral EBSPs should preclude any possibility for direct or indirect sharing and transfer 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.

4.5. Data protection safeguards

56. The EDPS positively notes that the proposed negotiating directives include a number of safeguards, which the Commission as negotiator would aim to ensure in the future framework agreement. The EDPS specifically welcomes the objective for the agreement to provide safeguards and guarantees with regard to the protection of personal data and other fundamental rights and freedoms regardless of the nationality and place of residence of the individuals³⁴, which reflects the universal nature of the rights to privacy and data protection in the EU law.
57. Similarly, it is the understanding of the EDPS that the safeguards and the guarantees with regard to the protection of personal data and other fundamental rights and freedoms should apply independently of the purpose of the query. The EDPS believes that this is the right approach, given the specific nature of the exchanges under the EBSP, which are

³¹ See Explanatory Memorandum, COM(2025) 447 final, page 2.

³² For more information, see Regulation (EU) 2019/817 and Regulation (EU) 2019/818 ('Interoperability Regulations').

³³ Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, OJ L 135, 22.5.2019, pp. 1–26.

³⁴ See point 11 of the Annex, COM(2025) 447 final.

without precedent, and the potentially serious consequences for the affected data subjects in both the law enforcement and the immigration context, as already explained above.

58. Another important safeguard concerns the conditions triggering a query on a traveller. According to the proposed negotiating directives, the framework agreement should provide clear and precise rules and procedures that preclude a systematic, generalised and non-targeted processing of data for all travellers³⁵. While the EDPS welcomes and strongly supports this safeguard, he underlines the need to ensure that it is fully implemented in practice. To this end, the EDPS recommends including in the framework agreement effective accountability mechanisms, in particular an obligation for clear and specific justification of each query as well as logging of all processing operations related to the exchange.
59. The EDPS also welcomes the proposed safeguards regarding storage that limit the retention of travellers' personal data after their departure and its linking to objective evidence from which it may be inferred that there is a continuing risk to public security or public order³⁶; the rules on automated processing of personal data, including profiling³⁷; the prohibition of onward transfers of personal data to third countries or international organisations³⁸; the exhaustive list of the competent authorities in the U.S. to which the Member States may transfer personal data as well as a short description of their competences³⁹.
60. The EDPS also positively notes that according to point 15 of the Annex of the Recommendation, the transfer of additional/supplementary information to the U.S. side would only be possible with the explicit authorisation of the respective EU Member State.
61. The EDPS however considers that this safeguard should be further developed and therefore recommends that the framework agreement provide for a general legal possibility for EU Member States to refuse sharing or transferring of data to U.S. authorities in individual cases.

4.6. Transparency

62. The EDPS positively notes that point 11(g) of the Annex of the Recommendation requires that the framework agreement should lay down rules, inter alia, 'on information to be made available to individuals'.
63. The EDPS recalls that the right to information is of utmost importance as it allows the exercise of the other data protection rights, including the right to remedies, and ensures fair processing of the data⁴⁰.
64. The EDPS therefore stresses that the information to be made available to the data subjects about the envisaged sharing of data between the EU and the United States pursuant to the

³⁵ See point 3 of the Annex, COM(2025) 447 final.

³⁶ See point 11(c) of the Annex, COM(2025) 447 final.

³⁷ See point 11(h) of the Annex, COM(2025) 447 final.

³⁸ See point 11(j) of the Annex, COM(2025) 447 final.

³⁹ See point 11(b) of the Annex, COM(2025) 447 final.

⁴⁰ See judgment of the Court of Justice of 1 October 2015, Case C 201/14, *Smaranda a.o.*, ECLI:EU:C:2015:638, in particular para. 32 and 33 where the Court found that 'the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, and their right to object to the processing of those data' and '[t]hat information concerns the identity of the data controller, the purposes of the processing and any further information necessary to guarantee fair processing of the data'.

EBSP should be clear, easily accessible and sufficiently detailed to allow the individuals to be aware and to understand the purposes and the scope of the processing of their personal data, the identity of the data controller(s), the legal avenues for redress, and any other information necessary to ensure a fair and transparent processing of their data. Moreover, the EDPS reminds that the obligation about the transparency of the processing applies to both the U.S and the EU competent authorities.

4.7. Oversight and redress

65. The EDPS notes that, according to the proposed negotiating mandate, the framework agreement should ensure a system of oversight over the use of personal data by one or more independent bodies responsible for data protection in the U.S. with effective powers of investigation and intervention. In particular, the body or bodies should have powers to hear complaints from individuals about the use of their personal data. In addition, the framework agreement should also ensure enforceable rights of administrative and judicial redress for any person whose data are processed under the framework agreement and should guarantee effective remedies⁴¹.
66. In this regard, in line with Article 8(3) of the Charter and Article 16(2) TFEU, the EDPS stresses the importance of the existence of effective oversight and redress mechanisms, implemented by independent authorities. He is specifically concerned about the availability of judicial redress in the United States for all data subjects, irrespective of their citizenship and of the purpose of the data sharing. The EDPS recalls that the U.S. Judicial Redress Act of 2015 has extended certain rights of judicial redress established under the Privacy Act of 1974 to EU citizens. However, this extension is linked to the scope of application of EU-U.S. Umbrella Agreement, i.e. it is applicable only in case of transfers for law enforcement purposes. At the same time, as already explained in this Opinion, the envisaged personal scope of the framework agreement is much broader.
67. The EDPS therefore recommends that the framework agreement offers guarantees that all data subjects would be able to avail themselves of the right to judicial redress in the United States (under the U.S. Judicial Redress Act or a similar U.S. legal act), regardless of their citizenship and the purposes of the processing under the EBSP.
68. In addition, the EDPS notes that point 11(k) of the Annex of the Recommendation, which deals with oversight mechanisms, refers to ‘a duty of cooperation between such oversight bodies, on the one hand, and the relevant Union supervisory authorities, on the other hand’. The EDPS invites the Commission to clarify what is meant by ‘Union supervisory authorities’ and what exactly would be their role and obligations under the ‘duty of cooperation’.

5. Suspension and termination

69. The EDPS also positively notes that the proposed negotiating directives foresees an explicit provision in the framework agreement whereby a Party may terminate or suspend it, ‘in

⁴¹ See point 11(k) and (f) of the Annex, COM(2025) 447 final.

particular where the U.S. no longer effectively ensures the level of protection of fundamental rights and freedoms required under the framework agreement'⁴².

70. Given the complex nature of the proposed cooperation between the EU and the United States, comprising both a framework agreement at Union level and EBSPs at national level, the EDPS recommends that the possible suspension and termination of the framework agreement, especially in situations where the U.S. no longer effectively ensures the required level of protection of fundamental rights and freedoms, should entail similar suspension or termination of the bilateral agreements and arrangements concluded by EU Member States.

6. Conclusions

71. In light of the above, the EDPS urges the Commission and the Council to take into account the following specific recommendations:

- (1) *to conduct an in-depth fundamental rights impact assessment of the proposed framework agreement and the Enhanced Border Security Partnerships with the United States;*
- (2) *to consider the seriousness of the interference by the proposed sharing of personal data with a third country for the purposes of border and immigration control by the United States as being comparable to the seriousness of the interference caused by the exchanges of data for law enforcement purposes;*
- (3) *to define the personal scope of the framework agreement exhaustively and as narrowly as possible, taking also into account the specific prohibitions of data sharing laid down in EU law;*
- (4) *to clarify the notions of 'family members' and 'permanent residents';*
- (5) *to circumscribe exhaustively and as narrowly as possible the categories of personal data that may be exchanged under the framework agreement, including the content and the scope of the supplementary information to be provided to the U.S. authorities in case of a match, especially if the query is carried out for non-law enforcement purposes;*
- (6) *to preclude any possibility for direct or indirect sharing and transfer of data from the EU large-scale IT systems in the area of justice and home affairs and in particular from those related to migration and asylum;*
- (7) *to include in the framework agreement effective accountability mechanisms, in particular an obligation for clear and specific justification of each query, as well as logging of all processing operations related to the exchange;*
- (8) *to guarantee that the individuals would be provided with clear, easily accessible and sufficiently detailed information about the envisaged processing pursuant to the EBSP, to allow them to be aware and to understand the purposes and the scope of the processing of their personal data, the identity of the data controller(s), the legal avenues for redress, and any other information necessary to ensure a fair and transparent processing;*

⁴² See point 21 of the Annex, COM(2025) 447 final.

- (9) to provide for a general legal possibility for EU Member States to refuse sharing or transferring data to U.S. authorities in individual cases;*
- (10) to guarantee that all data subjects would be able to avail themselves of the right to judicial redress in the United States, regardless of their citizenship and the purposes of the processing under the EBSP;*
- (11) to clarify the meaning and the scope of the ‘duty of cooperation’ between supervisory authorities;*
- (12) to provide that the possible suspension and termination of the framework agreement, especially in situations where the U.S. no longer effectively ensures the required level of protection of fundamental rights and freedoms, would entail a similar suspension or termination of the bilateral agreements and arrangements concluded by EU Member States.*

Brussels, 17 September 2025

(e-signed)

Wojciech Rafał WIEWIÓROWSKI