Draft 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

A legal analysis by European Digital Rights

EDRi
European Digital Rights

EDRi's analysis of the leaked draft of the Framework Agreement for an Enhanced Border Security Partnership (EBSP) between the European Union and the United States finds that the text, as it stands, **is incompatible with EU data protection law and the Charter of Fundamental Rights**. Its provisions fail to guarantee the essentially equivalent level of protection that the Court of Justice of the European Union requires for international transfers of personal data.

If adopted in this or any similar form, the agreement **would severely undermine the rights to privacy and data protection, as well as the freedoms of movement, expression and assembly.** It would hand the the US government a powerful new tool to further target political dissidence and opposition – including that of people in the EU.

EDRi therefore calls on the European Commission and the Council to withstand pressure from the US administration and to refuse the transfer of individuals' personal data to a third country whose record of human rights violations and recent democratic backsliding raise serious concerns. The Commission **should suspend negotiations until the United States has remedied the shortcomings of its domestic legal framework with respect to data protection, fundamental rights and the rule of law. No agreement is better than an agreement that trades away fundamental rights.**

Published in Brussels, 20 July 2025.

Lead authors: Jesper Lund (IT-Pol Denmark) and Chloé Berthélémy (EDRi).

European Digital Rights (EDRi) thanks Romain Lanneau (Statewatch) and Pamela Valenti (EDRi) who supported with the review of this paper.

Table of Contents

1. Executive summary....4
2. Introduction....5
3. Outline of the envisaged information exchange in an EBSP agreement....7
3.1 First step: exchange on information through automated queries (Article 7)....8
3.1.1 Profiling based on social media monitoring and risk of discrimination based on political opinions....8
3.1.2 Automated data transfers from national information systems....9
3.2 Exchange of indications of risk (Article 8)....10
3.2.1 Adoption of US standards to define "risks"....10
3.2.2 Severe consequences of automated information transfers about "risks" without human review....11
3.3 Second step: further exchange of additional information (Article 9)....12
4. Legal analysis of the privacy and data protection aspects of the draft Framework Agreement....12
4.1 Preliminary remark: EU's essential equivalence criteria and authorisation in each Party's law for third country transfers of personal data....13
4.2 Proportionality of the interference with fundamental rights....14
4.3 Clarity and precision of conditions for risk assessment....14
4.4 Purpose limitation (Article 12)....15
4.5 Onward transfers within the US (Article 13)....16
4.6 Proportionality of data retention periods (Article 19)....16
4.7 Sensitive personal data (Article 20)....17
4.8 Data subject rights....17
4.8.1 Data accuracy, right to access and rectification (Articles 15, 22 and 23)....17
4.8.2 Access to remedies (Article 24)....18
4.8.3 Right to notification (Article 25)....19
4.8.4 Automated decision-making (Article 21)....19
4.9 Data protection oversight by independent authorities (Article 26)....20
4.10 Suspension of transfers by data protection authorities (Article 29)....21
5. Comparison of the Framework Agreement text with the negotiating directives adopted by the Council....22
6. Conclusion....25
7. Acronyms....25

1. Executive summary

On 1 May 2026, the draft text of the Framework Agreement for an Enhanced Border Security Partnership (EBSP) between the European Union (EU) and the United States (US) was leaked. This future international agreement aims to set out the modalities of the information exchange and rules on processing of personal data between the US and EU Member States for the purpose of screening and identity verification of travellers. It foresees the automated exchange of personal data, including biometric data, as well as of risk assessment. Since 2022, the US has made it a new requirement for countries wishing to keep visa exemptions for their citizens.

According to European Digital Rights (EDRi), the draft Framework Agreement currently poses two major problems: (1) it diverges significantly from the Member States' negotiating directives adopted in December 2025; (2) its provisions are, in large parts, not compliant with EU primary and secondary law, notably the Charter of Fundamental Rights.

The draft Framework Agreement falls short of meeting EU data protection requirements, including the requirement of reaching an essentially equivalent level of protection for international transfers, in the following ways:

1. **Non-compliance with the principle of proportionality:** EBSP data exchange entails a serious interference with the rights to privacy and data protection but its purposes include the fight against non-serious threats to public security or public order. Therefore, the interference with fundamental rights is disproportionate to the intended purpose.

2. **Lack of legal clarity and precision of rules for risk assessment:** the text does not sufficiently define the conditions for carrying out and sharing risk assessment in the first step of the process, whereas the requirement of near real-time transfer limits the possibilities for human intervention and strongly incentivises the use of automation.

3. **Excessive data retention**: The draft does not limit the retention of personal data to what is strictly necessary, since no maximum retention period is specified. Even after the traveller's departure from the US, the Department of Homeland Security (DHS) could store the data for up to 75 years.

4. **Lack of adequate safeguards for automated decision-making:** there is no requirement for meaningful human intervention in each case involving automated decision-making and it is impossible for data subjects to request one, as they are usually not aware they were subjected to automated decision-making.

5. **Undermining of the principle of purpose limitation**: the draft deems as compatible purposes any further processing by law enforcement authorities for any criminal investigations and by administrative authorities, where the processing is "linked to the facts stemming from the assessment of the travel" application or border checks. Not only are those conditions overly broad and vague, but the unrestricted further processing by law enforcement authorities completely undermines the principle of purpose limitation enshrined in EU law.

6. **Weak data protection enforcement for US state-level law enforcement**: US federal

authorities can share EBSP data with local authorities, but the data protection requirements do not apply to them. The envisaged oversight and enforcement mechanisms are inadequate and severely restricted.

7. **Lack of guarantees for data subject rights and remedies**: Restrictions on the right to notification and access, as well as redress options for data subjects are subject exclusively to US law. Moreover,the preamble specifies that it is not mandatory to offer each type of remedy available under US law in every instance – which is contrary to the CJEU case law (C-362/14, *Schrems*). While the US Judicial Redress Act is not applicable to EBSP data transfers and the US standing doctrine *de facto* excludes affected individuals from accessing effective judicial remedies, the draft Framework Agreement fails to oblige the US government to appoint or establish dedicated bodies for judicial redress.
8. **Lack of independence of oversight and complaint mechanisms:** according to the draft, data protection oversight powers would be exercised exclusively within the scope of U.S. law, i.e. by existing bodies that are not required to be independent of government interference and have proved to be highly controlled by the Trump administration.
9. **Suspension hardly actionable by EU data protection authorities**: suspending the agreement in case of breach is only possible after 'a reasonable period of consultation without reaching a resolution' has passed. This undermines the independence of EU Member States' data protection authorities, as they cannot suspend transfers without their government's consent.

If adopted in its current state, **the draft Framework Agreement risks being invalidated if subjected to judicial review, for it conflicts with several EU data protection legal criteria** as per CJEU jurisprudence.

Furthermore, the draft Framework Agreement enables the transfer of third country nationals' data processed by EU Member States, even though they would not be eligible for visa exemption – thus creating an unfair treatment among EU citizens and residents, in contradiction with the universal character of the rights to private and family life and data protection under the Charter.

EDRi calls on the Commission and the Council to resist the US government's pressure and refrain from transferring individuals' personal data to a third country whose record of human rights violations and recent democratic backsliding raise serious concerns.

2. Introduction

The United States (US) has introduced Enhanced Border Security Partnership (EBSP) agreements as a new requirement for countries participating in its Visa Waiver Program (VWP). This includes all European Union (EU) Member States, except Bulgaria, Cyprus and Romania. The purpose of the EBSP is automated exchange of personal data, including biometric data, for screening and identity verification (vetting) of travellers.

The US demands for greater information access about travellers has parallels to 2009, where conclusion of Preventing and Combatting Serious Crime (PCSC) agreements was made a precondition for continued VWP participation. The PCSC agreements allow for exchange of fingerprint and DNA data in criminal investigations similar to the Prüm framework (automated searches of biometric databases of other Member States with hit/no-hit response).

Unlike the existing PCSC agreements, information exchange under the future EBSP will not be connected to specific criminal investigations since the purpose is a general "security screening" of travellers before they enter the US. This means that sensitive personal data about a large number of individuals could be transferred to the US.

In the EU, EBSP agreements will consist of two parts: a Framework Agreement between the EU and US, which is currently being negotiated, and bilateral agreements between each Member State and the US. The Framework Agreement will set out the modalities of the information exchange and rules on processing of personal data. The bilateral agreements will determine the specific national databases from which information can be exchanged with the US.

The Framework Agreement will be an international agreement of the EU, which is adopted by the Council by a qualified majority with the consent of the European Parliament (Article 218 TFEU). Council Decision 2025/2640 of 16 December 2025 nominates the Commission as negotiator on behalf o the Union and sets out the negotiating directives for the Commission in its annex. The annex has not been published, which is symptomatic of EBSP agreements being shrouded in secrecy. Only the draft annex of the Commission proposal for the Council Decision has been made publicly available.[1]

On 1 May 2026, European Digital Rights (EDRi) member Statewatch published a Council document with the draft text of Framework Agreement and provided an initial analysis.[2] In the Council document, dated 16 April 2026, the draft text is described as "the agreement in principle reached at lead negotiators' level."[3]

---

1 Based on leaked Council documents with amendments to the Commission proposal, as well a Euractiv news article providing access to the adopted text of the annex, EDRi has reasons to believe that the 2025 Council decision does not depart significantly from the text in the Commission proposal [COM(2025) 447 final].
European Commission, 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, COM/2025/447 final, 23 July 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0447
Maximilian Henning and Nicoletta Ionta, 'EXCLUSIVE: US algorithms judging EU travellers not fully excluded in draft data deal', *Euractiv*, 20 February 2026, https://www.euractiv.com/news/exclusive-us-algorithms-judging-eu-travellers-not-fully-excluded-in-draft-data-deal/

2 Romain Lanneau, 'EU-US data exchange proposal in conflict with EU laws', Statewatch, 1 May 2026, https://statewatch.org/analyses/2026/eu-us-data-exchange-proposal-in-conflict-with-eu-laws/

3 According to the Council Document Register, a second revised text (WK 9138/26) exists and has been sent to Member States on 22 June 2026. EDRi will update this legal analysis, if needed, when revised texts of the Framework Agreement are leaked.

This analysis by EDRi assesses whether the draft text of the Framework Agreement complies with EU data protection law and the Charter of Fundamental Rights. The analysis also considers whether the negotiating result meets the demands and expectations of Member States, as outlined in the negotiating directives and (leaked) Council documents.[4]

Whilst the EBSP agreement is reciprocal, and allows EU Member States to obtain information from US databases about travellers bound for the EU, EDRi's analysis focuses on situations where US authorities conduct automatic searches of databases in Member States, and where Member States provide additional information to the US as follow-up to these searches. These cases entail transfer of personal data to the US, a country that, in our view, does not provide an essentially equivalent level of protection to EU law.

However, it should be noted that, despite the official connection between concluding an EBSP agreement with the US and participating in the VWP, **the information exchange will also cover third country nationals that are not eligible for visa exemptions. Thereby, their personal data effectively becomes a bargaining chip for securing visa-free travel for EU citizens.**

3. Outline of the envisaged information exchange in an EBSP agreement

The description in the following sections is based on the draft Framework Agreement text and the Department of Homeland Security's (DHS) Privacy Impact Assessment[5] describing the processing of personal data under EBSP from the perspective of US border authorities.

The EBSP information exchange process has certain similarities to the Prüm II Regulation, as it foresees an automated response to queries in the first step and a follow-up procedure for exchange of additional information related to the match.[6]

Personal data can be exchanged for the purposes of identity verification and for the screening and vetting of individuals needed to determine whether their entry or stay would pose a genuine risk to public security or public order (Article 6). This allows data exchange for a broad list of purposes, which immediately raises questions about its proportionality and conformity with EU data protection law. The Trump administration's interpretation of political opposition and dissent to the US government as risks to "public order" raises serious human rights concerns.[7]

---

4 https://www.statewatch.org/media/5205/eu-council-ebsp-recommendation-decision-third-compromise-wk-15766-25.pdf
https://www.statewatch.org/media/5204/eu-council-ebsp-negotiations-note-16362-25.pdf

5 Privacy Impact Assessment Update for the DHS International Biometric Information Sharing (IBIS) Program – Enhanced Border Security Partnership (EBSP), DHS/ALL/PIA-095(b), 26 April 2024
Privacy Impact Assessment for the DHS International Biometric Information Sharing (IBIS) Program, DHS/ALL/PIA-095, 2 November 2022, https://www.dhs.gov/publication/dhsallpia-095-international-biometric-information-sharing-program-ibis

6 See section 3.3, European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes. Position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II"), 7 September 2022, https://edri.org/wp-content/uploads/2022/10/EDRi-position-paper-Respecting-fundamental-rights-in-the-cross-border-investigation-of-serious-crimes-7-September-2022.pdf

7 The US State Department has launched an AI-based "Catch and Revoke" initiative which scrapes social media for alleged expressions of support for Hamas or others designated as 'terrorist groups'. The initiative is believed to have resulted in hundreds of arrests and student visa revocations of peaceful pro-Palestinian protesters. See Morgan

3.1 First step: exchange on information through automated queries (Article 7)

Under the future EBSP agreement, when a person would be applying for a travel authorisation (ESTA) or visa, or during a border check, US competent authorities would be able to submit an automated query to EU Member States in relation to that individual, if there is "reason to believe" that the person will pose a genuine risk to public security or public order. US authorities cannot submit automated queries on every person seeking to travel to the US, as the Framework Agreement specifically refers to a maximum volume of individuals to be screened. However, this limitation appears to be mostly justified by technical capacity constraints, rather than due consideration for the necessity and proportionality principles.[8]

3.1.1 Profiling based on social media monitoring and risk of discrimination based on political opinions

As "reason to believe", Article 7(1) mentions indicators of identity fraud, authenticity of travel documents, false information in visa applications and prior information in US information systems about the person, as well as more generic reasons such as "risk assessments and scenarios identifying risk on the basis of experience, trend analysis of suspicious activity" and "patterns identified".

All travellers to the US are profiled in the Automated Targeting System (ATS) which collates information from US law enforcement and border control databases, DHS watchlists, Passenger Name Records (PNR) data from air carriers, commercial data brokers and social media.[9] Visa applications to the US must contain social media identifiers, and the privacy setting for the profiles must be set to "public".[10] For travel authorisation (ESTA) applications, providing social media identifiers is currently optional, but the DHS announced its intention to make it mandatory.[11] The ATS

McCann, "Catch & Revoke: How Trump's AI is Silencing Student Activism," The American University International Law Review https://auilr.org/2026/01/27/catch-revoke-how-trumps-ai-is-silencing-student-activism/
There are also news reports of scientists being denied entry to the US due to their personal opinions on Trump, see e.g. Clea Caulcutt, "French academic denied entry to US for 'personal opinion' on Trump", *Politico*, 20 March 2025 https://www.politico.eu/article/france-academic-denied-entry-united-states-donald-trump-personal-opinion-messages/
Lastly, the 2026 US Counterterrorism Strategy indicates that the government's priorities will include "the identification and neutralisation of violent secular political groups whose ideology is anti-American, radically pro-transgender, and anarchist". See https://www.whitehouse.gov/wp-content/uploads/2026/05/2026-USCT-Strategy-1.pdf

8 According to Article 1(5), the information exchange shall be based on a "maximum volume of individuals to be screened, taking into account the capacity and technical limitations of the Competent Authorities, real volumes of travel, current risks, and reciprocity, to the extent determined in the bilateral agreements."

9 Systems of Record Notice (SORN) for DHS/CBP-006-Automated Targeting System, 22 May 2012 (the most recent) https://www.federalregister.gov/documents/2012/05/22/2012-12396/privacy-act-of-1974-us-customs-and-border-protection-dhscbp-006-automated-targeting-system-system-of
The Privacy Impact Assessments for ATS (see https://www.dhs.gov/publication/automated-targeting-system-ats-update) contain information about data sources which have been added after 2012, e.g. commercial data brokers and social media.

10 State Department, Announcement of Expanded Screening and Vetting for Visa Applicants, 18 June, 2025 https://www.state.gov/releases/office-of-the-spokesperson/2025/06/announcement-of-expanded-screening-and-vetting-for-visa-applicants/

11 The US Customs and Border Protection (CBP) posted a notice in the Federal Register on 10 December 2025 about planned changes to the ESTA application which include mandatory declaration of social media accounts used by applicants, see https://www.federalregister.gov/d/2025-22461/page-57209 As motivation for making social media identifiers mandatory, the CBP refers to compliance with the January 2025 Executive Order 14161 (Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats). As of 30 June 2026, the announced planned changed to ESTA have not yet been implemented.

Privacy Impact Assessment published by DHS highlights the vital role of social media data for screening of travellers.[12]

US authorities could therefore screen the social media profiles of **all travellers** in the ATS, since this is not prohibited by the Framework Agreement, and use this analysis to single out individuals for automated queries under the EBSP, which does include a capacity limit.

Article 7(2) prohibits arbitrary and unjustifiable discrimination on the grounds of "sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation." The blatant absence of "**political opinions" from the list of protected grounds**[13] would turn any forms of opposition to the Trump administration, support to transgender people's rights[14] or protests against the genocide in Gaza expressed (publicly) on social media into "permitted" reasons for US authorities to query EU Member States' databases under the EBSP Framework Agreement.

3.1.2 Automated data transfers from national information systems

The automated query can be based on:

- Identity information included in the application or in travel documents, such as name, date of birth, national ID number, and/or
- the fingerprint of an individual.

The specific national information systems to be searched in the Requested State will be specified in the bilateral EBSP agreements (Article 5). The information systems should ideally contain what is referred in the preamble as "identity information, including possible criminal history as well as security risk indicators". In a Privacy Impact Assessment Update for EBSP, the DHS gives an indication of the types of databases that the US is interested in querying:[15]

- Biographic information (civil registration databases)
- Known criminal convictions and arrests for serious crime[16] (police records)
- Indications of the individual's immigration status in the country.

12 Privacy Impact Assessment Update for the Automated Targeting System DHS/CBP/PIA-006(e), 13 January 2017 (updated December 2024), https://www.dhs.gov/sites/default/files/2024-12/24_1210_priv-pia-cbp-automatedtargetingsystem006-appendixupdate.pdf
The social media analysis includes link analysis to identify direct contacts (such as friends, followers and likes), as well as secondary and tertiary contacts associated with the applicant that pose a potential risk to the US or demonstrate a nefarious affiliation on the part of the applicant. Information related to each of these contacts may be retained in ATS and used in the vetting process. See the Privacy Impact Assessment Update for the Electronic System for Travel Authorization (ESTA), DHS/CBP/PIA-007(g), 1 September 2016, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-september2016.pdf
This suggests that the vetting process could also use social media information obtained through other ESTA applications. It could be linked to an applicant not providing social media identifiers themselves through their phone number or email address.

13 Unlike Article 20 about processing special categories of personal data where political opinions is included in the list of data items.

14 Diana Nerozzi, Trump counterterrorism strategy targets 'violent left-wing extremists' with 'transgender ideology', *Politico*, 5 June 2026, https://www.politico.com/news/2026/05/06/trump-counterterrorism-strategy-vows-to-counter-violent-left-wing-extremists-with-transgender-ideology-00909284

15 Privacy Impact Assessment Update for DHS International Biometric Information Sharing (IBIS) Program – Enhanced Border Security Partnership (EBSP), DHS/ALL/PIA-095(b) https://www.dhs.gov/sites/default/files/2024-04/24_0429_priv_pia-dhs-all-095b.pdf

16 The US definition of "serious crime" is a crime that is considered a felony under US law (maximum custodial sentence of one year or more).

The Framework Agreement specifically refers to **national** information systems. This excludes EU information systems in the Justice and Home Affairs (JHA) area managed by eu-LISA from the scope of EBSP agreements with the US, as the legal acts regulating these systems generally prohibit transferring information to third countries.[17] However, if the information from EU systems was replicated in e.g. national immigration systems, it would then be possible to exchange it with the US under the EBSP – which would de facto circumvent this important safeguard applicable to EU databases.

An automated query can be submitted if there is a nexus between the individual and the Requested State, i.e. citizenship, residence status or previous stays in the territory of the Requested State. The Framework Agreement does not seek to establish a mechanism similar to the Prüm II central router.[18] However, nothing prevents the US from establishing an infrastructure for searching databases of multiple EU MS simultaneously, as long as the bilateral capacity limits are respected.[19]

The Requested Competent Authority must respond to queries in "near real-time". In case of a match in the queried information systems, the Requested Competent Authority **must respond through the automated process** with a confirmation of the match and, where available, photographs of the individual and biographic information (such as full name and date of birth).

It is noteworthy that the automated response to the match must include not only a confirmation of the match, but also **additional information about the individual**. In the Prüm system, the automated response only includes a confirmation of the match. Any additional information in the Prüm system (core data) is exchanged through the follow-up process, where the Requested State has time to scrutinise and possibly refuse the request. **This means that the EBSP would provide a more extensive data exchange framework between the US and individual Member States than between two Member States**.[20]

3.2 Exchange of indications of risk (Article 8)

In case of a match found during the automated query, the Requested Competent Authority must immediately assess, based on all relevant factors (including criminal convictions, national security and terrorist threats and immigration violations), whether the match is related to a risk set forth in Article 6. The wording "all relevant factors" suggests that the Requested Competent Authority is expected to search additional databases for information about the individual, on top of the ones automatically queried in the first step.

---

17 As pointed out by the European Data Protection Supervisor in paragraph 54 of his opinion 24/2025, 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 nationals stored in Eurodac. Article 18 of Regulation (EU) 2019/816 (ECRIS-TCN Regulation) prohibits sharing of information about criminal convictions of third-country nationals and stateless persons stored in the European Criminal Records Information System.

18 Since the last revision of the Prüm framework, the exchange of personal data is supposed to take place under a new IT architecture including a central router to which national databases connect, replacing the former model where bilateral connections between each national database were necessary. This central router has not yet been implemented at the time of writing. See Regulation (EU) 2024/982 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), https://eur-lex.europa.eu/eli/reg/2024/982/oj/eng

19 The US has EBSP agreements with other states and is seeking agreements with (at least) all VWP countries. It is not known whether these agreements have capacity limits for automated searches (the agreements are not publicly available).

20 The EBSP will also be more extensive than the existing PCSC agreements between the US and Member States.

The sharing of indications of risk with the Requesting Competent Authority can only take place if this is authorised by bilateral agreements, and only according to the procedures established in those bilateral agreements. This may expose Member States to pressure from the US to include similar provisions in their bilateral EBSP agreements.

3.2.1 Adoption of US standards to define "risks"

Since the "risks set forth in Article 6" are determined by the Requesting State for its screening of travellers and can include broadly defined risks to public order, **the wording of Article 8 could be interpreted as an obligation for the Requested EU Member State to effectively conduct a risk assessment of the individual according to criteria set by the US government. The adoption of US standards to define "risks" is highly problematic and potentially against EU primary law, in light of the US government's growing criminalisation and repression of freedom of expression and assembly.**[21] Participation in a public protest against the genocide in Gaza should not in itself be regarded as an "indication of risk", even if the person was somehow registered by domestic authorities. However, the Trump administration has shown to have a different perspective on this matter, considering the recent immigration crackdown on peaceful pro-Palestinian protesters at university campuses[22] under the guise of protecting "public order".[23]

3.2.2 Severe consequences of automated information transfers about "risks" without human review

The indications of risk **must be shared in near real-time** if the query is submitted at the borders, and 'without delay' in other cases (visa and travel authorisation applications). The very short response time for sharing risk indications means that there will be little or no possibility for meaningful human review, assessment of necessity, data minimisation or verification of the information.

First, data collected by law enforcement and national security services about individuals, which could be used for risk assessment under the EBSP, is frequently of dubious quality. Police databases are notoriously plagued by poor quality data, allegations relying largely on hearsay or consisting of information that cannot be verified, e.g. provided by other authorities or other states.[24] **These problems with data quality will be further exacerbated when the information, or parts thereof (indications of risk), is transferred to competent authorities in another state where it will be inevitably interpreted in a different context and for different purposes than the original collection.**

Second, meaningful human review by the Requested State will be completely impossible for queries taking place at the border as long as the indications of risk must be provided in near real-time. In this situation, where the response from the Requested State will be *de facto* automated, the consequences of inaccurate information can be particularly severe for the person concerned, as they may be detained by US border authorities based on flawed indications of risk provided by an EU Member State.

The draft Framework Agreement does not restrict the actions that Requesting Competent

---

21 Whitney Bauck, The criminalizing of protest and dissent has a long history in America, *The Guardian*, 3 February 2026, https://www.theguardian.com/us-news/2026/feb/03/criminalizing-protest-dissent-history

22 Al Jazeera Staff and Reuters, US reinstates deportation proceedings against Mohsen Mahdawi, 7 May 2026, https://www.aljazeera.com/news/2026/5/7/us-reinstates-deportation-proceedings-against-mohsen-mahdawi

23 The US White House, Protecting The American People Against Invasion, 20 January 2025, https://www.whitehouse.gov/presidential-actions/2025/01/protecting-the-american-people-against-invasion/

24 European Digital Rights, Respecting fundamental rights in the cross-border investigation of serious crimes A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II"),

Authorities (e.g. US border authorities) may take based on the information exchanged. The Framework Agreement even allows decisions "producing significant adverse actions concerning the relevant interests of individuals" **to be taken solely based on automated processing (i.e. without human involvement)**, as long as this is permitted by legal framework of the Party (Article 21). The broad wording for automated decision making in Article 21 can cover physical detention at the border as well as refusal to grant a travel authorisation or visa.[25]

3.3 Second step: further exchange of additional information (Article 9)

Article 9 of the draft Framework Agreement provides for exchange of additional information in case of a match in the automated query (first step, Article 7). At this stage, additional information will likely already have been shared in an automated manner through the procedure in Article 8 (indications of risk).

The second step of the information exchange is closer to traditional Mutual Legal Assistance (MLA) procedures than other parts of the EBSP Framework Agreement. The exchange of additional information may only take place to the extent authorised by the bilateral agreements, and only after a human assessment of compliance with those conditions, in accordance with applicable domestic law. This corresponds to the normal procedure in MLA agreements.

It is noteworthy that, through Article 9, the Framework Agreements allows for effective human review in the information exchange process for the first time. Neither the completely automated response in Article 7, which would confirm the match and include additional biographic information and facial images (biometric data), nor the *de facto* automated sharing of indications of risk under Article 8 provide for a meaningful human assessment by competent authorities in the Requested State or the possibility to refuse requests.

Article 11 includes a general non-derogation clause, which permits the Requested State to refuse requests pursuant to a bilateral agreement or arrangements or if the response would conflict with applicable domestic law or international obligations. However, the very tight deadlines for automated responses in Articles 7 and 8 would severely limit, if not eliminate, the possibilities for the Requested State to actually use any applicable grounds for refusal in these situations.

4. Legal analysis of the privacy and data protection aspects of the draft Framework Agreement

This legal analysis of the Framework Agreement focuses on the provisions that would determine whether the agreement ensures an essentially equivalent level of protection when personal data is

25 Whilst the refusal of a visa or travel authorisation (ESTA) can entail serious interference with fundamental rights, e.g. the right to family life if seeking to visit relatives in the US, the economic well-being of the person if travel to the US is a professional necessity, or exercise of the right to freedom of assembly in international political gatherings, the immediate consequences for the person concerned are still significantly greater if the actions of competent authorities involve physical detention at the border. Often limited procedural rights are afforded to the individual who can be detained for a prolonged period until released or deported. In the US, border detention facilities are frequently operated by private contractors who have a vested financial interest in prolonging the detention. Under the second Trump administration, there have been numerous news reports of travellers from Europe and elsewhere being detained by US border authorities for lengthy periods under dismal conditions due to alleged minor irregularities. See for the example Louis Oelofse, Germany 'monitoring' US detentions of its citizens, *Deutsche Welle*, 17 March 2025 https://www.dw.com/en/germany-monitoring-us-detentions-of-its-citizens/a-71952116

transferred to the US. The underlying premise of the analysis below is that the draft Framework Agreement will facilitate a **systematic transfer of personal data to the US**. Whereas, admittedly, there would not be information exchange about every travellers from the EU to the US, the draft Framework Agreement gives US authorities essentially unfettered access to select individual travellers for screening, only within the limits of(unspecified technical capacity constraints.

Moreover, the envisaged EBSP information exchange must be analysed in the context of other surveillance measures against travellers by US authorities, in particular the opaque screening of their social media profiles (which all travellers are expected to provide information about when applying for a visa or travel authorisation[26]). Whilst the social media screening takes places outside the EBSP framework (and does not involve transfers of personal data from Member States' authorities), **the consequences for fundamental rights of travellers, including the risk of discrimination, could be exacerbated by the subsequent information exchange within the EBSP framework.**

4.1 Preliminary remark: EU's essential equivalence criteria and authorisation in each Party's law for third country transfers of personal data

The US does not have a legal framework on data protection and the Commission has not adopted any adequacy decisions on the EU for transfers of personal data to law enforcement or border and immigration control authorities.[27]

To address the lack of legal frameworks on the protection of personal data in the US, Part 3 of the draft Framework Agreement contains some data protection provisions on personal data transferred under the bilateral EBSP agreements with EU Member States that will be binding on the US Federal Government (Articles 12-26).

Most articles under Part 3 reflect the wording of the corresponding articles in the 2016 EU-US Umbrella Agreement on the protection of personal information exchanged for the purpose of prevention, detection, investigation and prosecution of criminal offences.[28] However, there are some notable differences.[29] The Umbrella Agreement includes a provision on cooperation between US and EU data protection authorities that finds no correspondence in in Part 3. Moreover, the provisions on purpose limitation are considerably weaker in the EBSP Framework Agreement, especially on administrative and judicial redress.

The data protection rules in the draft Framework Agreements (outlined below) are intended to provide appropriate safeguards for third country transfers within the meaning of the GDPR and LED.

26 Providing social media profiles is mandatory for visa application. For travel authorisation (ESTA), it is currently optional, but the intention to make it mandatory for ESTA has been announced in December 2025, see footnote 11. .

27 The Data Privacy Framework adequacy decision covers transfer of personal data to private companies. The Umbrella Agreement between the US and the EU, which is not an adequacy decision but is intended to provide appropriate safeguards within the meaning of Article 37(1)(a) LED, does not cover transfers of personal data for border and immigration control purposes. With regards to the latter, it should be noted that the joint review of the Umbrella Agreement, in line with its Article 23 and due in 2020, still has not been finalised. See https://www.europarl.europa.eu/doceo/document/E-9-2020-004472_EN.html

28 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, available at: https://data.europa.eu/eli/agree_internation/2016/2220/oj

29 A complete comparison between Part 3 of the EBSP Framework Agreement and the Umbrella Agreement is outside the scope of this legal analysis. However, since the Umbrella Agreement is been subject to considerable criticism for not ensuring sufficient protection when personal data is transferred to the US, the overall conclusion that the Framework Agreement offers a weaker protection is highly relevant.

This follows from Article 4(3), which states that by giving effect to the data protection provisions, the processing of personal data by Competent Authorities "shall be deemed to comply with their respective data protection legislation **restricting or conditioning international transfers of personal information, and no further authorisation under such legislation shall be required.**" (emphasis added).

The Second Additional Protocol to the Council of Europe Cybercrime Convention uses the same approach for authorising third country transfers in State Parties with data protection laws.[30] If the Receiving State has implemented the data protection provisions in Article 14 for personal data received under the Protocol, the Transferring State cannot refuse transfers for reasons of data protection under its own legal framework.[31]

Since the draft Framework Agreement prohibits Member States from refusing transfers of personal data to the US for reasons of data protection, it is critical to assess whether the data protection rules (Part 3) in the draft Framework Agreement provide an essentially equivalent level of protection, as required by the case law of the Court of Justice of the European Union (CJEU).

4.2 Proportionality of the interference with fundamental rights

Databases in EU Member States can be searched based on biometric data (fingerprints), and the automated response to database queries in case of a match includes biometric data (facial images), if available. Moreover, the Requested State must immediately assess the risk of the individual concerned and provide indications of risk according to criteria set forth by the US. This processing is likely to involve **profiling of the individual**, and the indications of risk transferred will be used for further risk assessment by US authorities, possibly by automated analysis without human intervention. **The personal data to be transferred undeniably entails a serious interference with fundamental rights of the person concerned.** This indirectly affects all travellers to the US insofar as they do not know whether their personal data will be transferred to the US, nor are they likely to be informed about the "indications of risk" that Member States' authorities could potentially share with the US.

In its judgment on the PNR Directive C-817/19 *Ligue des droits humains v Conseil des ministres*, the CJEU considers the following elements to constitute serious interferences with fundamental rights: systematic transfer of personal data, transfer of sensitive personal data, long retention periods and the use of the transferred personal data for risk assessment.[32] **All elements are present in the EBSP draft Framework Agreement.**

Under the principle of proportionality, the objective pursued by the limitation of fundamental rights must be proportionate to the seriousness of the interference. International PNR agreements of the EU have the objective of combatting terrorism and serious crime, which under CJEU case law can justify serious interferences. However, the objective of the EBSP is identity verification as well as

30 See Article 14, paragraph 1 d, Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, 12 May 2022, https://rm.coe.int/1680a49dab

31 Article 14(1)(d) of the Second Additional Protocol. See European Digital Rights, Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention. Why is the opinion of the Court of Justice of the European Union necessary?, 13 April 2022, https://edri.org/wp-content/uploads/2022/04/EDRi-Position-Ratification-EU-Member-States-Cybercrime-Second-Additional-Protocol.pdf .

32 See Meijers Committee, Comment on EU–US negotiations for an enhanced border security partnership on the exchange of personal data for border procedures and visa applications, 8 May 2026, https://www.commissie-meijers.nl/comment/meijers-committee-comment-on-eu-us-negotiations-for-an-enhanced-border-security-partnership-on-the-exchange-of-personal-data-for-border-procedures-and-visa-applications/

screening and vetting of travellers to determine whether they would pose a risk to public security or public order. **Since this objective is considerably broader than terrorism and serious crime, and covers non-serious threats to public security or public order, the interference with fundamental rights does not appear to respect the principle of proportionality.**

4.3 Clarity and precision of conditions for risk assessment

It is also unclear whether the rules for processing personal data under the draft Framework Agreement are **sufficiently clear and precise.** Recently, a case was referred to the CJEU to clarify whether the ETIAS Regulation 2018/1240 specifies the purpose of assessing security risks with sufficient precision.[33] Similarly to Article 3(1)(6) ETIAS, which broadly defines a security risk as the "risk of a threat to public policy, internal security or international relations for any of the Member States", the expansive notion of risk assessment purpose under Article 6 of the draft Framework Agreement would most likely require clarification through judicial review.

The ETIAS Regulation has more detailed rules on processing personal data in the automated risk assessment than the draft Framework Agreement. For example, the ETIAS Regulation enumerates the databases that can be searched for "hits" about the applicant, whereas Article 20(5) specifies the data points about the applicant that must be compared with the risk indicators in Article 33(4).[34] For the EBSP, t**he list of databases to be searched on a hit/no-hit basis in the automated query under Article 7 is not precisely defined by the draft Framework Agreement**, leaving room for the US to define specific lists of databases in their bilateral agreements with Member States. In case of a match, the Requested State would then be obliged to share **indications of risk** under Article 8, which would require further database searches and analysis. **The draft Framework Agreement fails to clarify the exact rules and procedures for this additional processing.**

4.4 Purpose limitation (Article 12)

EU data protection law requires that personal data is collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes.

Personal data in the EBSP is collected for identity verification and screening of travellers in the context of border and immigration control. Under EU law, such processing falls under the scope of the GDPR, not of the Law Enforcement Directive (LED). If personal data collected for border control is to be further processed for law enforcement purposes, national or Union law must provide for a specific legal basis for this processing, which generally cannot be regarded as compatible with the original purpose (border control) and its legal basis. In addition, the legal basis for further processing by law enforcement must comply with Article 52(1) of the Charter of Fundamental Rights, which enshrines the principle of proportionality. This principle prevents unfettered access by law enforcement to all personal data collected for border control.[35]

---

33 Case C-846/25, *Ligue des droits humains*.

34 In EDRi's opinion, the ETIAS Regulation entails a general and indiscriminate data collection and risk assessment analysis about all visa-exempt travellers to the EU, potentially through error-prone and discriminatory AI algorithms, which is not limited to what is strictly necessary, and does not respect the principle of proportionality enshrined in Article 52(1) of the Charter. However, the ETIAS Regulation is not the object of this legal analysis. It is only included here to document that the EBSP Framework Agreement has data processing rules which are less precise than the ETIAS Regulation, which is subject to a legal challenge before the CJEU.

35 For example, law enforcement access to the ETIAS system is limited to investigations of terrorism or serious crime, and there are further substantive and procedural conditions for access, as well as limitations on what data can be obtained from the ETIAS system for law enforcement purposes (see ETIAS Regulation 2018/1240, Chapter X). Similar

The Framework Agreement includes a provision specifying that personal data must not be further processed for an incompatible purpose. However, paragraph 3 of Article 12 prescribes compatible purposes in relation to law enforcement to include "processing for criminal investigations and proceedings" and "preventing an immediate and serious threat to public security". It also contemplates any further processing by administrative authorities, where the processing is "linked to the facts stemming from the assessment of the application" for travel authorisation or border checks, as compatible.

As pointed out by the European Data Protection Supervisor (EDPS) in paragraph 19 of his Opinion 24/2025 on the EBSP negotiating mandate, there is a divergent understanding between the EU and the US of the boundaries between processing of personal data for border control and processing personal data for law enforcement.

The limits imposed on further processing of personal data in the US are not sufficiently specified, and are therefore unlikely to satisfy the Court's case law. In its Opinion 1/15, the CJEU found that some provisions for further processing in the envisaged EU-Canada Passenger Name Record (PNR) agreement were "too vague and general to meet the requirements as to the clarity and precision required".

The first compatible purpose **covers any processing for criminal investigations** without limitations or substantive conditions. Thereby, its overly broad scope appears to violate the principle of proportionality. **By granting a blank cheque for repurposing to law enforcement without any substantive or procedural conditions, the draft Framework Agreement effectively allows for a complete conflation of border control and law enforcement purposes on the US side.**

In light of this highly expansive notion of repurposing, the lack of restrictions on further processing by law enforcement authorities blatantly counters the principle of purpose limitation as enshrined in EU law.

4.5 Onward transfers within the US (Article 13)

The draft Framework Agreement states in Article 13(1) that processing of personal data by other national law enforcement, regulatory and administrative authorities shall respect its data protection provisions.

However, the draft Framework Agreement would only be legally binding for the US Federal Government, not for subsidiary bodies such as law enforcement authorities at state level. Article 13(2) requires the US Government to "promote accountability" for other national authorities that are not covered by the draft Framework Agreement, and to address "serious misconduct" through appropriate measures, such as discontinuation of transfers, if these authorities are found not to have effectively protected personal data.

However, such weak standards of data protection enforcement standards are inadequate, insofar as they fail to ensure compliance with data protection rules by non-federal authorities. Under these circumstances, individuals whose personal data have been transferred would have no enforceable rights in cases of onward transfers within the US. Furthermore, the obligation for the US Government to address misconduct is only limited to *serious* misconduct, which creates substantial risks of repeated violations of the fundamental right to data protection. **The striking absence of appropriate without any accountability mechanisms fails to ensure a an essentially equivalent**

restrictions on law enforcement access exist in other EU instruments on border control and migration., such as Eurodac and the Common Identity Repository (CIR).

level of protection.

4.6 Proportionality of data retention periods (Article 19)

Since **no maximum retention period is specified in the draft agreement**, the draft Framework Agreement falls short of limiting the retention of personal data to what is strictly necessary. Furthermore, it allows for the transferred personal data to be retained after the passenger's departure from the US, even in the absence of objective evidence indicating that the passenger may continue to constitute a risk to public security or public order.

Article 19 merely requires Parties to establish specific retention periods in their applicable legal framework to ensure that personal data is not retained for longer than is necessary and appropriate. This represents a **materially lower level of protection than what is permissible under EU law**, which permits the retention of personal data only where it is demonstrably necessary and proportionate to a legitimate objective.

On the US side, personal data received under the EBSP would be stored in the Automated Targeting System (ATS) which, according to information provided by the DHS, retains personal data for **up to 75 years.** Such retention period which is **manifestly disproportionate** when assessed against the principles of necessity and proportionality that govern the retention of personal data under the EU data protection framework.[36]

4.7 Sensitive personal data (Article 20)

While replicating the definition of sensitive personal data enshrined in EU law under the GDPR and LED, which includes biometric data for the purpose of uniquely identifying a natural person, the draft Framework Agreement adds that the processing of sensitive personal data must take place "under appropriate safeguards in accordance with law." However, the examples of "appropriate safeguards" listed under Article 20(2) correspond to general safeguards that would apply to any processing of personal data under the GDPR or LED . This fails to ensure stronger safeguards for the processing of sensitive data in compliance with EU law. This is all the more particularly problematic as the EBSP Framework Agreement allows for the systematic transfer of biometric data to the US.

4.8 Data subject rights

4.8.1 Data accuracy, right to access and rectification (Articles 15, 22 and 23)

The GDPR and LED require that personal data shall be accurate and, where necessary, kept up-to-date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

The seemingly corresponding provision under Article 15 of the draft Framework Agreement is, in fact, considerably weaker, as the Requesting and Requested Competent Authority are only required to advise the other Party if they "become aware of significant doubts" about the accuracy of personal data received or transferred.

36 According to the SORN for ATS (see footnote 8), the retention period for the official records maintained in ATS will not exceed 15 years. However, DHS processes personal data in many other systems. The Privacy Impact Assessments for ATS and IBIS/EBSP indicate a DHS retention period of 75 years for biometric and biographic records, see the Privacy Impact Assessment for 'DHS International Biometric Information Sharing (IBIS) Program – Enhanced Border Security Partnership (EBSP)', DHS/ALL/PIA-095(b), pp. 8-9.

The main obligation for the controller to rectify inaccurate personal data is linked to the data subject exercising their rights to access and rectification under Article 22 and 23. However, the data subject's exercise of the right to access and rectification would be challenging in practice.

The draft Framework Agreement requires Parties to ensure that individuals can obtain access to their personal data from a Competent Authority and rectify it in accordance with the applicable legal framework of the State in which access is sought (Articles 22 and 23). When personal data is transferred to the US, the right of access would follow the conditions and procedures that are provided for under US law. **The Framework Agreement's failure to guarantee that the right of access will be free of charge for the individual** is a major weakness of the draft text, which merely provides that "excessive expenses" shall not be imposed on the individual.

In addition, the grounds for restricting data subject rights under Article 22(2) are far broader than those permitted under the GDPR and LED. For example, the excessively vague ground for restricting the right of access set out Article 22(2) (f) (i.e. where the restriction "otherwise protects interests provided for in legislation...") has no equivalent in EU law. Furthermore, the draft text also fails to recognise that any restrictions of the right of access must respect the essence of fundamental rights and freedoms and, in accordance with EU law, must be necessary and proportionate in a democratic society to safeguard objectives of general interest, such as the prevention, investigation, detection or prosecution of criminal offences.

The Framework Agreement does not specify which US legal framework would apply to data subject requests. Whereas the US Privacy Act provides a right for individuals to access records about themselves, this right is only applicable to US citizens and residents. Moreover, federal agencies can exempt themselves from almost all requirements in the Privacy Act, as extensively demonstrated by the DHS with regards to the Automated Targeting System.[37]

In 2015, the Judicial Redress Act extended certain data subject rights established in the Privacy Act to EU citizens (third country nationals remain excluded). However, the extension only applies to personal data transfer for the purpose of preventing, investigating, detecting, or prosecuting criminal offences.[38] Since the EBSP governs personal data transfers for identity verification and screening procedures in the context of border procedures and applications for travel authorisations or visas, EU citizens are excluded from the scope of the Judicial Redress Act for transfers under the draft Framework Agreement.

The only legal avenue available for data subject requests under the EBSP would be the US Freedom of Information Act (FOIA) which, in principle, also covers access to records containing the individual's personal data. However, when access has been exempted under the Privacy Act or other exemptions, the access under FOIA will be restricted as well.[39]

Therefore, **the existing US legal framework provides no effective data subject rights for personal data transferred under the EBSP**.[40]

---

37 Edward Hasbrouch, Why the Judicial Redress Act is worthless, 25 February 2016, The Identity Project https://papersplease.org/wp/2016/02/25/why-the-judicial-redress-act-is-worthless/

38 See definition of covered record in Section 2(h)(4)(B) of the Judicial Redress Act of 2015, 5 U.S.C. § 552a note https://www.govtrack.us/congress/bills/114/hr1428/text

39 See recital 118 of the Commission Implementing Decision EU 2023/1795 for the adequacy decision under the EU-US Data Privacy Framework.

40 One way to address this limitation would be for the US Government to establish data subject rights via an Executive Order, which will be legally binding on federal agencies, similar to the EU-US Data Privacy Framework. There is no indication in the Framework Agreement that this approach will be used.

4.8.2 Access to remedies (Article 24)

When the right of access is denied for specific reasons after an individual assessment or for general reasons due to blanket restrictions, **EU law requires that the individual must have access to remedies**. The CJEU ruled in paragraph 95 of C-362/14 Schrems that legislation not providing for any possibility for individuals to pursue legal remedies in order to have access to their own personal data would be contrary to the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.

Article 24 requires Parties to "have in place effective administrative and judicial remedies to provide redress" for individuals whose personal data has been processed and used in a manner inconsistent with Part 3 of the draft Framework Agreement (data protection). The access to remedies is determined entirely by each Party's respective legal framework, with no minimum requirements imposed by the draft Framework Agreement. In the preamble, the Parties (EU and US) acknowledge that "it is for each Party to determine the type of remedies available, and that it is not required that each type of remedy be available in every instance."

In order to seek judicial redress in the US, the individual must demonstrate standing under Article III of the US Constitution, which requires that the individual has suffered a concrete "injury in fact". Because of the standing doctrine, the individual will, in many cases, not have access to an effective remedy before a tribunal, as required by Article 47 of the Charter.[41] This includes notably cases where the data subject is not aware of the processing due to lack of individual notice, as highlighted by the experts assessments presented to the Irish High Court in paragraphs 222-238 of the judgment *Data Protection Commissioner v Facebook Ireland Ltd*.[42]

The EU-US Data Privacy Framework seeks to address the limitations of the standing doctrine with the Data Protection Review Court, which is established through an Executive Order.[43] The Framework Agreement does not contain any obligation on the US government to establish similar bodies for judicial redress.

4.8.3 Right to notification (Article 25)

Article 25 requires Parties to ensure that notice is provided to individuals whose personal data is processed. However, this requirement can be met through publication of a general notice. The US government publishes notices about processing of personal data in the Federal Register (SORN). These notices are only sporadically updated and may be incomplete regarding the current data collection and processing. Moreover, the notices do not provide information for the data subject in "a concise, transparent, intelligible and easily accessible form, using clear and plain language", as required by Article 12 GDPR and Article 12 LED.

Data subject rights must be enforceable in practice, not just on paper. If individuals are not aware that their personal data have been transferred to the US and processed for risk assessment purposes, they will not be able to exercise their data subjects rights. The transparency obligations of

41 Theodore Christakis, Kenneth Propp, and Peter Swire, 'EU/US Adequacy Negotiations and the Redress Challenge: Whether a New U.S. Statute is Necessary to Produce an Essentially Equivalent Solution', European Law Blog, 31 January 2022, https://doi.org/10.21428/9885764c.e13321c1

42 The Data Protection Commissioner -v- Facebook Ireland Limited & anor, [2017] IEHC 545, https://www.bailii.org/ie/cases/IEHC/2017/H545.html

43 There is considerable controversy whether establishment of an administrative body within the Department of Justice through an Executive Order meets the requirement for an effective remedy before an independent and impartial tribunal in Article 47 of the Charter. See noyb, EU-US Data Transfers: Time to prepare for more trouble to come, 10 December 2025, https://noyb.eu/en/eu-us-data-transfers-time-prepare-more-trouble-come

the Framework Agreement could be met by publishing a general notice about the processing. However, **the CJEU has consistently emphasised the importance of individual notification as a precondition for individuals to be able to to exercise their data subject rights and have access to an effective remedy before a tribunal**.[44]

4.8.4 Automated decision-making (Article 21)

Article 21 allows for automated decision-making that may produce significant adverse consequences on the relevant interests of individuals *if* there are safeguards that include the possibility to obtain human intervention. However, the data subject will **generally not be aware that they are being subjected to an automated decision under the EBSP**.

In the judgment on the PNR Directive C-817/19 *Ligue des droits humains v Conseil des ministres*, the CJEU highlighted that the human intervention for the automated risk assessment must be put in the conditions to understand the reasons for a positive match. Without such meaningful human review, **the data subject may be deprived of their right to an effective judicial remedy** as enshrined in Article 47 of the Charter. However, given the requirement to share risk assessment outcomes in near real-time for cases at the border, the EBSP precludes the possibility for meaningful human review.

In line with CJEU jurisprudence, this provision is likely to contravene EU law, notably Article 22 General Data Protection Regulation (GDPR) and Article 11 Law Enforcement Directive (LED) as well as Article 47 of the Charter.

4.9 Data protection oversight by independent authorities (Article 26)

For essential equivalence, the third country should ensure effective independent data protection supervision, as required by Article 8(3) of the Charter, and should provide for cooperation mechanisms with the Member States' data protection authorities.

Article 26 of the draft Framework Agreement requires Parties to have in place one or more public oversight authorities that (a) exercise independent oversight functions and powers, (b) have the power to accept and act upon complaints from individuals and (c) have the powers to refer violations of law related to Part 3 of the draft Framework Agreement for prosecution or disciplinary action.

The only requirement of independence for point (a) refers to general oversight. The authority tasked with receiving complaints from individuals is not required to be independent and could be acting under instruction of the US Government. Moreover, the draft Framework Agreement leaves it to US law or policies to determine what the obligation to "act upon complaints" would entail, and fails to include a specific obligation for the authority to investigate a complaint. For these reasons, **the draft provisions related to oversight and individual remedies fall short of EU standards for essential equivalence.**

On 29 June 2026, the US Supreme Court in Trump v. Slaughter gave the President broad authority to remove Commissioners of the Federal Trade Commission, a regulatory agency assumed to be independent in the Commission's GDPR adequacy decision on the US (Data Privacy Framework). Relying on the "unitary executive theory", the Supreme Court ruled that independent executive authorities in the US are unconstitutional.[45] The ruling from the Supreme Court casts considerable

44 For example, paragraph 220 in Opinion 1/15 on the EU-Canada PNR agreement and paragraph 120 of C-548/21 *Bezirkshauptmannschaft Landeck*.

45 noyb, 'US Supreme Court just blew up EU-US Data Transfers', 29 June 2026, https://noyb.eu/en/us-supreme-court-

doubt on whether it will be possible at all to secure independent oversight of personal data transferred to the US in the context of the EBSP or other data transfer mechanisms.[46]

4.10 Suspension of transfers by data protection authorities (Article 29)

The possibility to suspend the Framework Agreement in the event of a material breach of the agreement is only envisioned in a generic clause under Article 29. Whilst this, in principle, includes the data protection provisions in Part 3, the suspension can be triggered only after the Parties have engaged in a reasonable period of consultation without reaching a resolution.

This undermines the independence of EU Member States' data protection authorities, insofar as they would not be allowed to suspend transfers without the agreement of the government of their Member State.

In summary, several elements of the draft Framework Agreement indicate that the envisaged transfer and processing of personal data for risk assessment of travellers in the EBSP would not comply with EU data protection law and the Charter of Fundamental Rights.

just-blew-eu-us-data-transfers

46 EDRi and al.,The credibility of the EU's adequacy framework depends on action, not assumption, Letter to Ursula von der Leyen, President of the European Commission and Michael Michael McGrath, EU Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, 14 July 2026, https://edri.org/wp-content/uploads/2026/07/The_credibility_of_the_EUs_adequacy_framework.pdf

5. Comparison of the Framework Agreement text with the negotiating directives adopted by the Council

This section compares the draft Framework Agreement text with the negotiating directives for the Commission and other positions on the EBSP expressed by Member States in Council documents.[47]

Member States' negotiating directives	Draft Framework Agreement
Targeted searches	
Member States wanted clear and precise rules and procedures for triggering a query on a traveller in individual cases, to preclude a systematic, generalised and non-targeted processing of data for all travellers.	The draft allows queries to be submitted based on opaque "reason to believe" criteria which leaves a lot of discretion to US authorities. The safeguards against unlawful discrimination are also inadequate (e.g. based on political opinions). The selection of travellers for screening under EBSP will likely be based on an even more opaque social media surveillance by US authorities. The only hard limit preventing monitoring of all travellers is the unknown (technical) capacity limit of automated database searches.
Data access in the first step (hit/no-hit searches)	
Member States wanted a two-step procedure like the Prüm framework, where the automatic response should include limited personal data allowing identification of the person, and additional information is only shared with explicit authorisation of the Requested Party.	In the negotiated text, Member States would, in case of a match (hit), be required to immediately conduct a risk assessment of the person concerned and share risk indications with the US as part of the initial information exchange. The very short response time for sharing risk indications does not allow for meaningful human review, which makes the sharing of risk indications automated in practice. The initial data exchange goes considerably beyond the mere sharing of biographic data as in the Prüm framework.

47 The adopted negotiating directives have not been published, so the analysis will be based on the draft directives in the Commission proposal for a Council Decision and information available a news article with access to the non-public negotiating directives. The other Council documents included in the analysis are: 10444/24, WK 11360/25, WK 15766/25 and, 16362/25 (all published by Statewatch).

Data retention periods	
Member States wanted retention of travellers' personal data after their departure from the US to be limited to persons, where there is objective evidence of a continuing risk to public security or public order. The CJEU Opinion 1/15 on the EU-Canada PNR agreement highlighted this requirement to limit retention of personal data to what was strictly necessary.	The draft leaves data retention entirely to US law and policies. DHS will store the transferred personal data in the Automated Targeting System (ATS), where personal data is retained up to 75 years.
Sensitive personal data	
In the negotiating directives, the transfer of sensitive personal data should only be allowed where strictly necessary and proportionate in individual cases.	In the draft, the automated response to first-step queries includes transfer of biometric data (facial images) by default. The rules on processing of sensitive personal data in the draft Framework Agreement do not limit this processing to what is strictly necessary.
Automated decisions without human involvements	
Member States wanted to prohibit decisions based solely on automated processing without human involvement. Neither the PNR Directive nor the ETIAS Regulation allows automated decisions without human review.	The negotiated text allows automated decisions without human review if authorised by US law.
Purpose limitation and further processing	
Personal data is transferred for the purpose of identity verification and screening of travellers in connection with border crossings. In the negotiating directives, onward transfers of personal data to other authorities in the US should only be allowed for the purposes of the Framework Agreement and should be subject to the consent of the Member State which provided the information.	In the negotiated text, any further processing by law enforcement authorities in the US is deemed a compatible purpose, and the personal data can be transferred to local authorities in the US that will not be bound by the data protection requirements of the Framework Agreement.
Data protection oversight and redress	
The negotiating directives outline a system of oversight by one or more independent bodies responsible for data protection in the US with effective powers of investigation and	The negotiated text leaves data protection oversight and powers entirely to US law and policies, most likely through existing bodies that are not required to be independent of the

intervention. In particular, the bodies should have the powers to hear complaints from individuals.[48] The US bodies should have a duty of cooperation with relevant supervisory authorities in the EU.	US Government. There is no obligation to cooperate with data protection authorities in the EU. Access to remedies will be entirely according to US law and policies, and the negotiated text suggests that remedies may only be available if there is an individual concern based on data exchange with the US, which would be almost impossible for an individual to prove since the exchange of data is done in secret.

6. Conclusion

In summary, when negotiating the Framework Agreement text with the US, **the Commission has reneged on most essential requirements set by Member States in the negotiating directives**.

The negotiated text seems to almost entirely reflect US demands for unfettered information access, as articulated in DHS documents on the EBSP and International Biometric Information Sharing (IBIS) programmes.

Moreover, the negotiated text allows for a level of information exchange with the US that goes beyond the information exchange between Member States in the Prüm system and other JHA cooperation mechanisms. Member States have no obligation to conduct risk assessments of individuals on their territory, but producing and sharing such information with the US on extremely short notice will be a requirement in the EBSP.

It is extremely worrying that the Commission has negotiated an agreement that could facilitate systematic transfers of biometric data and highly sensitive (and subjective) risk indications about individuals to the Trump administration, which has shown a blatant disregard for basic human rights through harsh and inhumane treatment of migrants and visitors.

48 In light of the US having no data protection law at the federal level, this would likely require new specialised bodies to e.g. hear complaints from and provide redress options to individuals whose personal data has been transferred, similar to the Data Privacy Framework agreement which is the legal underpinning of the Commission's adequacy decision on the US. The judgement of the US Supreme Court in Trump v Slaughter takes away any remaining doubts on the lack of independence of data protection supervisory authorities that can be dismissed at will by the US executive.

7. Acronyms

ATS	Automated Targeting System
CBP	Customs and Border Protection
CJEU	Court of Justice of the European Union
DHS	Department of Homeland Security
EBSP	Enhanced Border Security Partnership
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights
ESTA	Electronic System for Travel Authorisation
EU	European Union
GDPR	General Data Protection Regulation
IBIS	International Biometric Information Sharing
JHA	Justice and Home Affairs
LED	Law Enforcement Directive
MLA	Mutual Legal Assistance
PCSC	Preventing and Combatting Serious Crime
PNR	Passenger Name Records
SORN	System of Records Notice
US	United States
VWP	Visa Waiver Program

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us

Rue Belliard 12
1040 Brussels
Belgium

Follow us

Mastodon
Facebook
LinkedIn
Youtube
Instagram

EDRi
European Digital Rights