To:
Members of the Council Working Party on JHA Information Exchange (IXIM)
Members of the Council Working Party on Visa (VISA)

CC:
Anu Talus, European Data Protection Board Chair (EDPB)
Wojciech Wiewiórowski, European Data Protection Supervisor (EDPS)
Members of the Civil Liberties, Justice and Home Affairs Committee of the European Parliament

20 July 2026

Dear Presidency, dear Attachés,

The undersigned civil society organisations, independent researchers and academics would like to draw your attention to the **worrying direction taken by the European Commission in the negotiation with the United States of America (US) on a Framework Agreement on the exchange of information for security screenings and identity verification relating to border procedures and applications for visa**.

We are concerned that the European Commission is seriously deviating from its negotiating mandate granted by the Council on 16 December 2025 by giving in to US demands in blatant violations of EU law. We attach to this letter a mapping of the divergences between the Council Decision and the latest available draft.[1]

Furthermore, **we call on the Council to push back against the excessive demands of the US Government**, which can be seen as nothing less than pressure tactics, **and uphold vital EU legal protections**. People's personal data, especially their biometric data, should not be up for sale, especially to a country responsible for increasing human rights violations and with a fast democratic backsliding.

1 We understand that a third revised draft text (WK 10195 2026 INIT) is available but due to the opacity of the negotiations process, we are limited in our comments to the latest version available, which is WK 5183/2026 INIT, See https://statewatch.org/wp-content/uploads/2026/05/wk_5183_2026pdf.pdf

Contradictions with EU law

On the basis of the leaked revised draft text (WK 5183/2026 INIT)[2], we are identifying the following discrepancies between the draft Framework Agreement and EU legal standards, including the requirement of reaching an essentially equivalent level of protection for international transfers:

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 purpose is not limited to serious crimes but includes a loosely defined threats to public security or public order. Therefore, the interference with fundamental rights cannot be considered proportionate.

2. **Lack of legal clarity and precision of rules for profiling:** the text does not sufficiently define the conditions for carrying out and sharing risk assessment, running the risk of unjustified profiling. Furthermore, the requirement of near real-time transfer implies automation with almost no possibility for human review, leaving no chances for individuals to understand why they have been profiled in the first place.

3. **AI-generated decision with no human review:** there is no requirement for meaningful human intervention in each case when using automated decision-making and it is impossible for data subjects to request one as they usually do not know they were subjected to it.

4. **Undermining of the purpose limitation principle**: information exchanged under this agreement could be used for any further processing by law enforcement authorities for any criminal investigation and by administrative authorities. Not only is it overly broad and does it give arbitrary powers to US law enforcement authorities, but the unrestricted further processing also completely undermines an essential principle of data protection law, the principle of purpose limitation.

5. **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. Department of Homeland Security (DHS) could store the data for up to 75 years.

6. **Weak data protection enforcement for US state-level law enforcement**: US authorities can share EBSP data with local authorities but the data protection requirements do not apply to them. The foreseen oversight and enforcement mechanisms are extremely poor and limited.

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 left entirely to US law and the preamble specifies that it is not mandatory to offer each type of remedy in every instance – which is contrary to 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 establish specific bodies for judicial redress.

2 Idem

8. **Lack of independence of oversight and complaint mechanisms:** the draft fails to require independent data protection oversight and powers from the US Government. As a result of actions taken by the Trump Administration and the U.S. Supreme Court, oversight bodies in the Executive Branch of the U.S. government are definitely not independent. The US Supreme Court's judgement in *Trump v Slaughter*, in which the executive was given the power to fire at will the head of the Federal Trade Commission, illustrates the lack of independence of any data protection authorities in the US.

9. **Suspension hardly actionable by EU data protection authorities**: suspending the agreement in case of breach can only be done after a reasonable period of consultation without reaching a resolution, which 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 not standing up in court, as it conflicts on many counts with EU data protection legal criteria, as interpreted by the CJEU.

Furthermore, the draft Framework Agreement enables the transfer of third country nationals' data processed by EU Member States, although they do not benefit from visa exemption – thus **creating an unfair treatment among EU citizens and third country nationals and in some cases EU citizens with a double nationality**, **in contradiction with the universal character of the rights to private and family life and data protection protected by the EU Charter of Fundamental Rights**.

Background

Since 2022, the US require the conclusion of Enhanced Border Security Partnership (EBSP) agreements with countries, including EU Member States, willing to remain part of its Visa Waiver Programme, granting visa exemption to their citizens. EBSP agreements imply the routine screening of travellers, asylum applicants or anyone encountered during US border screening and immigration procedures against the biometric databases of partner countries.

We thank you for your attention and remain at your disposal for any question you may have.
Sincerely,

Signatories:

Organisations:

Access Now
Alternatif Bilişim
Associació Pangea
Centre for Democracy and Technology Europe
Data Rights
Deutsche Vereinigung für Datenschutz e.V. (DVD)
Digitalcourage
Digitale Gesellschaft CH
Digitale Gesellschaft DE
Epicenter.works – for digital rights
European Digital Rights (EDRi)
European Sex Workers Rights Alliance (ESWA)
Hermes Center
Homo Digitalis

IT-Pol Denmark
La Quadrature du Net
Statewatch
Individuals:

Plixavra Vogiatzoglou, University of Amsterdam
Laurens Naudts, University of Amsterdam
Elisabetta Biasin, KU Leuven Centre for IT & IP Law
Dario Pronesti, KU Leuven Centre for IT & IP Law
Bilgesu Sumer, KU Leuven Centre for IT & IP Law
Sultan Erdogan, KU Leuven Centre for IT & IP Law
Sara Garsia, KU Leuven Centre for IT & IP Law
Raminta Matulytė, KU Leuven Centre for IT & IP Law
Catherine Jasserand, independent researcher
Maarten Hillebrandt, Utrecht University
Evelien Brouwer, Utrecht University
Annick Pijnenburg, Radboud University Nijmegen
Douwe Korff, London Metropolitan University

Annex: Comparison of the Framework Agreement draft text with the negotiating directives adopted by the Council

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.
Data retention periods	
Member States wanted retention of travellers' personal data after their	The draft leaves data retention entirely to US law and policies. DHS will store the

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.

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 intervention. In particular, the bodies should have the powers to hear complaints from individuals.[3] The US bodies should have a duty of cooperation with relevant supervisory authorities in the EU.

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 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.

3 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.