CM2608

# 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

May 2026

The Meijers Committee is concerned that the EU–US negotiations on a new data-exchange Framework Agreement pose major risks to the fundamental rights of data protection, non-discrimination and access to justice. The Meijers Committee emphasizes that the agreement could enable unprecedented large-scale transfers of sensitive personal data (including biometrics) for border and visa procedures without an impact assessment, both from third-country nationals as from EU citizens with double nationality. The Meijers Committee underlines that purpose limitation, data retention limits, data-subject rights, and safeguards against automated decision-making must be sufficiently guaranteed. Currently US oversight bodies are facing challenges to their independence. The Meijers Committee is also concerned about discriminatory effects of such transfer agreement. Personal data belonging to third-country nationals and EU nationals with dual nationality would be shared more extensively than that of EU citizens with a single nationality, without the "very weighty reasons" that European human-rights law requires to justify such differential treatment. The Meijers Committee notes possible gaps in the US legal system concerning the right to have access to justice, considering the limited scope of the current US Judicial Redress Act. Consequently, the Meijers Committee calls for a full data protection and human rights impact assessment before any agreement with the US is adopted.

Meijers Committee

Standing committee of experts on international immigration, refugee and criminal law

Meijers Committee

Introduction

With this comment, the Meijers Committee expresses its concerns regarding the ongoing negotiations on a Framework Agreement between the European Union (EU) and the United States (US) on the exchange of information for security screenings and identity verifications relating to border procedures and visa applications.[1] These negotiations take place within the context of the US Visa Waiver Program which requires the bilateral conclusion of Enhanced Border Security Partnerships (EBSP) between the US and EU Member States, enabling access to key national databases. As emphasized by the European Data Protection Supervisor (EDPS) in his Opinion 24/25, such an agreement would be unprecedented, as it would constitute the first EU agreement enabling large-scale sharing of personal data, including biometric data, for the purpose of border and immigration control with a third country.[2]

The Meijers Committee identifies specific legal problems concerning data protection, non-discrimination and access to justice, related to the adoption of the Framework Agreement. Therefore, it urges the EU legislator to provide sufficient guarantees protecting the fundamental rights of EU citizens and third-country nationals present within the EU. These safeguards must be in conformity with European legal standards, including the EU Charter on Fundamental Rights (CFR), the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED) and the AI Act. In line with this, the Framework Agreement should not grant individual Member States wide discretion to conclude bilateral data-transfer arrangements with the US in a way that could undermine these common EU fundamental rights standards in practice. Given the precedent-setting nature of the envisaged agreement, it is essential to ensure that any sharing and processing of personal data does not exceed the limits of what is strictly necessary and proportionate, as previously stressed by the EDPS.

## 1. Data Protection Standards

### 1.1. Impact Assessment

The negotiating directives for the above-mentioned Framework Agreement were not accompanied by an impact assessment even though they allow for a transfer of personal data, including biometric data, health data and other types of data that are considered sensitive under Article 9 of the GDPR and Article 10 of the LED. Impact assessments are required for legislative and non-legislative initiatives that are likely to have a significant economic, environmental or social impact or which entail significant spending and where the Commission has a choice of policy options.[3] In this context, non-legislative

[1] COM(2025) 447 final, 23.7.2025 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.
[2] EDPS Opinion 24/2025, 17 September 2025 https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2025-09-17-edps-opinion-242025-recommendation-council-authorising-opening-negotiations-framework-agreement-between-eu-and-usa-exchange-information_en.
[3] European Commission, Better Regulation Guidelines, SWD(2021) 305 final, 3 November 2021, p. 30.

initiatives include recommendations for the negotiations of international agreements.[4] Yet, the explanatory memorandum accompanying the negotiating directives states that "no impact assessment is required for the negotiation of this framework agreement" without further substantiating why the assessment is not necessary.[5] Considering the type of personal data involved, the Meijers Committee stresses the need for an impact assessment that shows the impact of EU-US data transfers under the Framework Agreement on individuals.

### 1.2. Strict Necessity Requirement

In accordance with Articles 7 and 8 CFR, interference with the right to private life and data protection must be limited to what is strictly necessary. This means that before developing new measures of data processing, the EU legislator should assess their necessity and define a clear and limited purpose for the use of the personal information.[6] The proportionality test to be applied must consider the seriousness of the interference. As identified by the CJEU, the following instances constitute serious interference: the systematic transfer of personal data; the extended scope of personal information to be transferred including sensitive data; long data retention periods; and the intended use of personal data for advanced and subsequent risk assessment of individuals.[7] Furthermore, the need for safeguards is all the greater where personal data is subject to automated processing and/or decisions and, considering the serious nature of these interferences with the right to private life and data protection, this will only be proportionate in limited necessary circumstances.[8]

### 1.3. Purpose Limitation

The Meijers Committee notes that based on the Framework Agreement, the boundaries between national powers for border management and immigration control on the one hand, and law enforcement and national security on the other hand, will be blurred. Without strict purpose limitation, US authorities may use personal data beyond the original stated purpose, depriving individuals of their right to foresee how and by which authorities their data will be used. The Meijers Committee notes that currently, it is still unclear which specific data will be shared, especially in the case of a "hit" in the database and requests for "supplementary" information. In this regard, the negotiating directives lack clarity about the content and scope of supplementary information, which seem to be left up entirely to be circumscribed in the bilateral arrangements.[9] This lack of specification of purposes will generate legal uncertainty, and is in violation of one of the core principles of EU data protection standards, including the principle of purpose limitation and data minimization.[10]

---

[4] See Impact Assessments on https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/impact-assessments_en.
[5] COM(2025) 447 final, p. 5.
[6] Joined cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärtner Landesregierung and Others [2014] ECLI:EU:C:2014:238; Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592.
[7] Case C-817/19 Ligue des droits humains v Conseil des ministres [2022] ECLI:EU:C:2022:491.
[8] Case C-817/19 Ligue des droits humains v Conseil des ministres, 115-117.
[9] EDPS Opinion 24/2025, 17 September 2025, para 42.
[10] Article 5 (1)(b) and (c) GDPR.

### 1.4. Data Retention Limits and Data Subject Rights

The Meijers Committee emphasizes the strict data retention periods applicable to the storage in EU law and applicable to the processing of personal data of both EU citizens and third-country nationals. These rules ensure that personal data are no longer retained than necessary (Article 5 (1) (e) GDPR) and in accordance with appropriate time limits (Article 5 LED). Any agreement with third states allowing for exchange of personal data with third states, should include obligations for the third state safeguarding these data retention limitations, offering at least the same protection as provided in the applicable EU legislation based on which these personal data have been collected and processed.

The same recommendation applies to the protection of data subject rights: any agreement with third states must ensure the protection of data subject rights as being protected in Articles 12-22 of the GDPR and Articles 12-18 of the LED.

### 1.5. Automated Queries and Decision Making

According to the Commission Recommendation, the Framework Agreement should provide for safeguards in respect of automated processing of personal data, including profiling and decision making, and should prohibit decisions based solely on the automated processing of personal data without human involvement.[11] The Commission does not clarify how to guarantee that these safeguards, as protected in both the GDPR and the AI Act, will be ensured with regard to automated queries, decision making and risk assessment by US authorities. The Meijers Committee emphasizes the responsibility of EU and national lawmakers and authorities to safeguard those rights for individuals whose personal data have been collected and stored based on EU laws and within EU territory. When transferring this personal data to third countries, the protection of these rights must be ensured as intended by the requirement of an adequate level of data protection that a receiving third country should comply with (Articles 36 LED and 45 GDPR). Lacking a general European Commission decision on adequacy, the EU and the US concluded the 2016 Umbrella Agreement ensuring compliance with EU data protection standards after data are transferred to US authorities.[12] These include a prohibition of automated decisions without human involvement but with an exception for those authorized under domestic law and with appropriate safeguards.

### 1.6. Independent Supervision Mechanism

In accordance with Article 8(3) CFR, the rules for processing of personal data must be monitored and enforced by an independent body. In the current EU-US Data Privacy Framework, the Federal Trade Commission (FTC) and the US Department of Transportation (DoT) are assigned this role in the US as independent bodies.[13] However, the independence of the FTC is currently under scrutiny as there is a US Supreme Court case pending regarding the removal of an FTC commissioner before their term

[11] COM(2025) 447 final, 23.7.2025 p. 3.
[12] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences ('Umbrella Agreement'), OJ L 336, 10.12.2016.
[13] Commission Implementing Decision EU 2023/1795 of 10 July 2023, Chapter 2.3.4 paragraph 59.

expired by the US President Donald Trump despite all independence guarantees.[14] If the Court rules in favor of the dismissal, the FTC's independence will be dismantled, and the requirement of an independent supervision body under the CFR will not be met anymore.

*Recommendations:*

- The proposed EU-US Data Transfer Agreement merits a prior impact assessment, including a substantiated justification for the proposed data transfers, which should entail a prior assessment of their strict necessity and proportionality. Such impact assessment should consider not only that sensitive data – including biometric data, genetic data, data revealing racial or ethnic origin, and health data – will be shared, but that this also includes the personal data of vulnerable persons, such as minors or asylum seekers.
- In line with the principles of necessity, proportionality, and data minimization, the categories of personal data to be exchanged should be circumscribed exhaustively and as narrowly as possible within the framework agreement, especially regarding the possibility of supplementary information being provided to the authorities of the third state as a result of a query for non-law enforcement purposes.[15]
- The Meijers Committee also urges for the inclusion of clearly defined purpose limitation provisions, as well as data retention limitation, and clearly defined individual rights of access, including the right to correction and deletion for the individuals whose personal data are being processed.
- The Meijers Committee urges the EU legislator to include in the data transfer agreement an obligation for US authorities to ensure the protection of the right to non-automated decision making (22 GDPR) and the right to explanation of the role of an AI system in the decision-making (86 AI Act) of individuals whose data have been transferred by EU institutions or EU Member States.
- Independent supervision of data processing is a key requirement under the GDPR and the LED and should be provided for clearly under the Framework Agreement. The independent bodies responsible for data protection located in the US should possess effective powers of investigation and intervention in accordance with the standards of EU data protection law.

2. Non-discrimination

While the objective of concluding bilateral arrangements envisages the sharing of information from national databases, it remains unclear which concrete data systems will be relied upon. At present, direct access to or transfer of data from certain EU-level databases may not be feasible within the timeframe of the envisaged negotiations and is in some cases restricted under existing legal frameworks. However, given the intention of establishing a comprehensive framework for EU–US data exchange, it cannot be excluded that, in the longer term, such cooperation could extend to one or

[14] Trump v. Slaughter (09/22/2025).
[15] See also the EDPS Opinion 24/2025, 17 September 2025.

more of the six large-scale EU data systems employed for the purpose of border and migration management (SIS, VIS, Eurodac, EES, ETIAS, ECRIS-TCN).

In any event, the categories of personal data to be shared, which include sensitive data such as biometric information, seem to disproportionately concern third-country nationals. The Meijers Committee is especially concerned that according to point 7 of the Annex of the Commission Recommendation, personal data of third-country nationals would be transferred for both immigration purposes ('in relation to the crossing of the external borders') and for law enforcement purposes ('in the context of the prevention, detection, investigation and prosecution of crimes and terrorist offences'). By contrast, in accordance with point 8 of the same Annex, personal data of [EU] citizens, their family members and of permanent residents may be exchanged only for law enforcement purposes, and only if 'strictly necessary and proportionate'. This distinction suggests that personal data of third-country nationals may be subject to broader conditions for transfer and comparatively weaker safeguards. This is particularly concerning in the foreseeable event that EU-level databases will be shared, as these primarily include biometrics on third-country nationals, and in ECRIS-TCN, even on EU citizens with a double nationality (both an EU and non-EU nationality).

According to settled case-law of the European Court of Human Rights (ECtHR) on the right to non-discrimination found under Article 14 of the European Convention of Human Rights (ECHR), different treatment of persons which is solely based on their nationality (or double nationality) requires very weighty reasons for justification.[16] The proposed differentiation in the Commission's Recommendation lacks a proper justification for this different treatment

*Recommendations:*

- The fact that data transfers with a third country will disproportionately affect third-country nationals or nationals with double nationality requires objective justification via a prior impact assessment. Upon the basis of the findings of this impact assessment, the Framework Agreement must clearly justify the necessity and proportionality of these measures and ensure that effective safeguards exist to prevent overextension. Without such justification, allowing said transfers of personal data amounts to a violation of the right to non-discrimination of the persons concerned (Article 21 CFR).
- It should be explicitly provided that regarding the exchange of personal data with US authorities, no different treatment solely based on the nationality of the data subject should be allowed, unless very weighty reasons have been provided. This non-discrimination clause should apply both to the definition of purposes for which data may be transferred and used, as well as the application of the 'strictly necessity' test.
- Moreover, the principle of non-discrimination must be strictly ensured in the context of large-scale automated processing of data and profiling risks. The Meijers Committee urges the EU

[16] ECtHR 16 September 1996, Gaygusuz/Austria, app.no. 17371/90, para 42; ECtHR (GC) 18 February 2009, app.no. 55707/00, Andrejeva/Latvia, para 87; ECtHR 5 December 2017, Ribać/Slovenia, app.no. 57101/10, para 53. See also our comment 'Creating second-class Union citizenship? Unequal treatment of Union citizens with dual nationality in ECRIS-TCN and the prohibition of discrimination', 10 April 2021.

legislator to include effective safeguards for meaningful human oversight within the Framework Agreement, capable of preventing and correcting biased or disproportionate outcomes.

3. Access to Justice – the Right to an Effective Remedy

The Meijers Committee has previously emphasized the necessity of safeguarding access to effective remedies for individuals, as protected in Article 47 CFR, whose personal data are being shared with third countries.[17] Whilst in the past, EU citizens as well as non-EU residents were excluded from the protection of the US Judicial Redress Act, a 2015 amendment has extended certain rights of judicial redress established under the Privacy Act of 1974 to EU citizens. However, this extension is insufficient within the context of the EU-US agreement under negotiation.

First, it only applies within the context of the 2016 EU-US Umbrella Agreement which concerns data transfers for the purpose of law enforcement. Therefore, data transfers for the purpose of border control management are not covered, yet under the proposed EU-US Framework, data transfers in the context of border control management will be the most frequent. Moreover, the US Judicial Redress Act does not protect third-country nationals affected by the implementation of the envisaged data transfer agreement, which includes non-EU citizens with a legal residence in the EU, visa applicants, asylum seekers, and those granted international protection. This means that if adopted, under the EU-US data transfer agreement, the US would not provide an equivalent level of protection to EU law and does not provide judicial redress for EU citizens, and even less for third country nationals.

Furthermore, the Meijers Committee stresses that there have been several legal cases regarding the adequacy of EU-U.S. data transfer agreements before the Court of Justice of the European Union. The *Schrems I* challenge invalidated the EU-U.S. Safe Harbor Framework in 2015 on the basis that it could not be ensured that the protection of the fundamental rights of data subjects provided in the US were 'essentially equivalent' to EU standards.[18] The second legal challenge led to the invalidation of the EU-U.S. Privacy Shield in 2020, partly due to a deficiency in safeguards on the power of US authorities and the inadequate recourse to an effective remedy.[19] In light of the Meijers Committee's abovementioned concerns, the Framework Agreement must provide for effective remedies and ensure that the level of protection provided is "essentially equivalent" to EU standards with respect to fundamental rights, to be compliant with the *Schrems* standard. Measuring proportionality by US standards rather than EU standards may thus jeopardize this Framework's compliance with EU law.

Although in 2025 the General Court of the EU dismissed action for annulment of the EU-US data transfer agreement (case *T-553/23 Latombe v. Commission),* the concerns about the adequate level of protection of personal data pursuant to Article 45 GDPR remain as the independent supervisory

[17] CM1613 Note on the Umbrella Agreement, 15 October 2016.
[18] C-362/14 *Schrems I* [71-74] [96].
[19] C-311/*18 Schrems II* [191].

body in the US is now being questioned. Aspects demanding scrutinization include President Trump's reliance on Executive Orders, which provide volatile ground for maintaining the independence of the FTC. An 18th February 2025 Executive Order requires several independent regulatory agencies including the FTC to submit significant regulatory actions to the President to be reviewed prior to their enactment, potentially inhibiting the functional independence of these bodies.[20]

Additionally, Trump's termination of all Democrat members of the Privacy and Civil Liberties Oversight Board (PCLOB) is obstructing it from functioning as an independent oversight body, noting that a quorum of three members is required for the Board to take formal action, yet only one member remains.[21] This includes its mandate to conduct an annual review of the Data Protection Framework redress mechanism, which is specifically mentioned as a means of independent evaluation in the EU's Adequacy Decision.[22] The role of the PCLOB is referenced in no less than 6 separate paragraphs of this Adequacy Decision; the present restriction in its functionality thus warrants serious contemplation of whether the Framework can still be considered adequate. Furthermore, in the *Latombe* judgment, the second argument, that the Data Protection Reviewing Court cannot be considered an independent and impartial tribunal, fell in part due to the observation that PCLOB is independent. It was noted that "[t]he independence of that agency is apparent from its composition. It is composed of a bipartisan, five-member board… for a fixed six-year term."[23] In the absence of all Democrat representatives, one may reasonably question whether this assertion will be maintained at appeal.

*Recommendations:*

- The Framework Agreement should ensure enforceable rights of redress for any person whose data are processed under the agreement and should guarantee effective remedies. This requires that the adoption of an EU-US agreement on the transfer of personal data should be made dependent on a prior extension by the US legislator of the protection of the Judicial Redress Act to any purpose for which personal data are being transferred to the US, including asylum, visa, and border management. Secondly, the scope of protection of the Judicial Redress Act should be extended to non-EU citizens whose personal data are being transferred by EU or national authorities to the US.

[20] Executive Order 14215, Ensuring Accountability for all Agencies, 18 February 2025.
[21] See How could Trump administration actions affect the EU-US Data Privacy Framework? | IAPP; Third Time's the Charm? The Fate of the EU–U.S. Data Privacy Framework - Berkeley Technology Law Journal; FISA Reauthorization Fearmongering and Disinformation Kicks Into Overdrive | Cato at Liberty Blog
[22] Commission Implementing Decision EU 2023/1795 [194].
[23] T-553/23 *Latombe v. Commission* [53].