WHITE PAPER

Data Privacy Framework Under Scrutiny:

Why You Should Reconsider Your EU-US Data Transfer Strategy Now

DPO Consultancy
Experts in Data Privacy

AUTHORS
Deniz Naz Kaya
Christos Stavrides

Data Privacy Framework Under Scrutiny: Why You Should Reconsider Your EU-US Data Transfer Strategy Now

Transferring data from the European Economic Area (EEA) to third countries – especially the Unites States (US) – remains one of the most legally contested and operationally critical issues which international businesses face today. Under the General Data Protection Regulation (GDPR),[1] such transfers must ensure a level of protection essentially equivalent to that guaranteed within the EU. The EU-US Data Privacy Framework (DPF), introduced to facilitate transatlantic data flows, now forms the backbone of many organisations' transfer strategies. However, with its legal durability under growing scrutiny and the shadow of past invalidations, namely Safe Harbour and Privacy Shield, businesses relying on the DPF face heightened regulatory uncertainty and risk. This paper outlines the legal foundations of the DPF, the lessons from past frameworks, and why businesses should reassess their data transfer strategies now, before the next disruption occurs.

The EU-US DPF, adopted on July 10, 2023, marks the European Commission's third attempt to legally safeguard transatlantic data flows, following the high-profile invalidation of its predecessors, Safe Harbour in 2015 (2015, *Schrems I*),[2] and Privacy Shield in 2020 (*Schrems II*),[3] by the Court of Justice of the European Union (CJEU).

Developed in response to deep concerns about US surveillance practices concerning bulk collection of personal data and the lack of enforceable rights for EU data subjects, the DPF promised stronger safeguards, clearer redress mechanisms, and closer oversight.

1 Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 27.04.2016 (GDPR)

2 Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6.10.2015, ECLI:EU:C:2015:650 (Schrems I)

3 Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 16.7.2020, ECLI:EU:C:2020:559 (Schrems II)

Yet less than two years later, the DPF is already facing intense scrutiny, from regulators, privacy advocates, and EU institutions alike. Political instability in the US, particularly the 2025 suspension of oversight by the Privacy and Civil Liberties Oversight Board (PCLOB), has raised serious concerns about the framework's long-term reliability.

As a result, businesses relying on the DPF as a stable legal mechanism for data transfers may be exposing themselves to regulatory, financial, and operational risks. This uncertainty has already translated into recent enforcement action. In one high-profile case, the Dutch Data Protection Authority (DPA) imposed a €290 million fine on Uber, underscoring the consequences of relying solely on unstable legal frameworks.

This white paper highlights critical US legal risks – particularly bulk data collection practices and the lack of enforceable rights for EU individuals – that reflect the same weaknesses which caused the failure of Safe Harbour and Privacy Shield. It assesses the likelihood of a Schrems III challenge and provides clear, practical steps businesses should take now to reduce risk and implement a reliable, GDPR-compliant contingency plan for transatlantic data transfers.

This white paper will address the following:

1. What Is the Legal Basis for the EU-US Data Privacy Framework?
2. What We Learned from Safe Harbour and Privacy Shield
3. Does the DPF offer "Essential Equivalent" Protection?
4. How US Political Instability Threatens the DPF
5. What happens if the DPF is invalidated – and What Should Businesses Do Now?

1. What Is the Legal Basis for the EU-US Data Privacy Framework?

The legal foundation for the EU-US DPF lies in the GDPR, which includes a dedicated chapter on the transfer of personal data to third countries or international organisations.[4] These provisions ensure that when personal data leaves the EEA, it continues to receive a level of protection "essentially equivalent" to that within the EU.

1.1 Adequacy Decisions Under the GDPR

One of the primary mechanisms to legitimise international data transfers under the GDPR is a formal adequacy decision,[5] issued by the European Commission. This means the Commission has reviewed the third country's legal framework, practices, and safeguards and concluded that these third countries provide a level of data protection that is "essentially equivalent" to that guaranteed within the EU.

The Court of Justice of the European Union (CJEU) has clarified that the standard is not identical regulation, but "essentially equivalent" protection in practice.[6] The European Commission maintains and periodically reviews a list of countries with adequacy status, available here.

Once adopted:

- No additional transfer mechanisms required.
- The transfer does not need prior approval from national DPAs.
- Supervisory Authorities (SAs) across the EU must recognise the decision, under Article 288(4) of the Treaty on the Functioning of the European Union (TFEU).

The Commission's adequacy is based on several criteria, including:

- Legal protections for privacy and data subject rights.
- Safeguards limiting public authority access to personal data.
- The presence of independent Supervisory Authorities.
- Enforceable data subjects' rights, including access, rectification and erasure.
- Participation in international agreements, particularly in relation to data protection.

4 GDPR Chapter V (Arts. 44-49)

5 GDPR Art. 45

6 Schrems I, para 73

1.2 Other Legal Transfer Mechanisms

Where no adequacy decision exists, organisations must rely on alternative transfer tools authorised under Chapter V of the GDPR. These include:

- Standard Contractual Clauses (SCCs): pre-approved contractual terms, published by the European Commission, to ensure data protection obligations are upheld by the data importer.[7]
- Binding Corporate Rules (BCRs): apply to multinational companies transferring data within their corporate group.[8]
- Specific derogations: applicable only in limited and exceptional situations (e.g. explicit consent or contract performance).[9]

These mechanisms often require additional safeguards, including Transfer Impact Assessments (TIAs), to evaluate potentially problematic national laws, both in theory and practice, securing effective protection for such transfers.

Want to Learn More?

For a more detailed overview of GDPR transfer tools – including when a transfer occurs, how SCCs should be implemented, and when TIAs are required – please refer to our companion white paper: **Transferring Personal Data to Countries Outside the EU: 5 Key Questions**.

1.3 The DPF as a Conditional Adequacy Decision

On 10 July 2023, the European Commission adopted an adequacy decision for the United States, specifically for US companies that choose to participate in the EU-US DPF.

However, this adequacy decision is limited in scope:

- It applies only to US organisations that self-certify under the DPF program.
- These organizations must fall under the jurisdiction of either the Federal Trade Commission (FTC) or the Department of Transportation (DoT).
- The decision is based primarily on safeguards introduced via Executive Order 14086 (EO 14086), which aims to restrict US intelligence access and introduce a redress mechanism for EU individuals.

Organizations outside the scope of FTC/DoT enforcement, such as banks, telecom providers, insurance companies, and non-profits, are not eligible to participate in the DPF. As such, the adequacy decision does not cover the entire US, but a specific, self-certified subset of commercial entities.

7 GDPR Art. 46

8 GDPR Art. 47

9 GDPR Art. 49

2. What We Learned from Safe Harbour and Privacy Shield

The EU-US Data Privacy Framework (DPF) follows two failed predecessors – Safe Harbour and Privacy Shield – both invalidated by the CJEU after legal challenges by privacy advocate Max Schrems. The rulings in Schrems I (2015) & Schrems II (2020) continue to shape adequacy standards and highlight persistent legal flaws in EU-US data transfers. Understanding these decisions is key to assessing the DPF's long-term viability.

2.1 *Schrems I (2015)*: Invalidation of Safe Harbour

In *Schrems I*, the CJEU ruled that the Safe Harbour framework failed to ensure an "essentially equivalent" protection of personal data. The Court identified several key shortcomings:

- **Unrestricted access:** US law permitted intelligence agencies to access EU personal data without limits that met EU standards of necessity and proportionality.[10]
- **Lack of redress:** EU individuals had no effective legal remedies in the US, violating Article 47 of the EU Charter of Fundamental Rights (The Charter).[11]
- **Bulk data collection:** The framework did not sufficiently restrict the mass collection of personal data by US authorities.[12]

As a result, CJEU invalidated the Commission's adequacy decision and required data transfers under Safe Harbour to be suspended without undue delay.

2.2 *Schrems II (2020)* – The Collapse of Privacy Shield

Following the invalidation of Safe Harbour, the European Commission adopted the Privacy Shield in 2015 to restore transatlantic data flows. It included commitments from US authorities and created an Ombudsperson mechanism to improve oversight and provide redress for EU individuals. However, in *Schrems II,* the CJEU ruled that these measures still failed to meet the EU's standards for protecting personal data. The CJEU pointed to several persistent and recurring weaknesses in US surveillance laws – like those identified in *Schrems I* – as well as the continued lack of effective legal remedies for EU individuals in the US.

10 Schrems I, para 93

11 Schrems I, para 95

12 Schrems I, para 94

The ruling focused on the following US law shortcomings:

US Surveillance Practices Remained Broad and Unchecked

- **Section 702 FISA** allowed US authorities to collect data from service providers (like cloud platforms) without individual court orders. The oversight was broad and general, not based on specific cases or precedent.
- **Executive Order 12333** permitted intelligence agencies to intercept data in transit, without any judicial prior-authorisation or oversight. The CJEU found this particularly concerning due to its virtually unlimited scope.[13]
- **Presidential Policy Directive (PPD-28)** introduced some privacy principles, but it was not legally binding and gave individuals no enforceable rights.[14]

No Effective Legal Remedies for EU Citizens

A core reason the Privacy Shield was struck down in *Schrems II* was that EU individuals had no meaningful way to challenge US government access to their personal data.

- **No access to US courts:** EU individuals lacked standing in US courts to challenge how their data was handled. US constitutional protection.[15]
- **Oversight lacked independence:** The Privacy Shield's Ombudsperson was part of the US State Department and could be removed by the President, hence not view as a tribunal within the meaning of Article 47 of the Charter.[16]
- **No enforceable rights:** The Court found that neither Section 702 FISA or EO 12333, provide individuals effective and enforceable rights, contrary to Art. 45(2)(a) GDPR.[17]

13 Schrems II, para 182

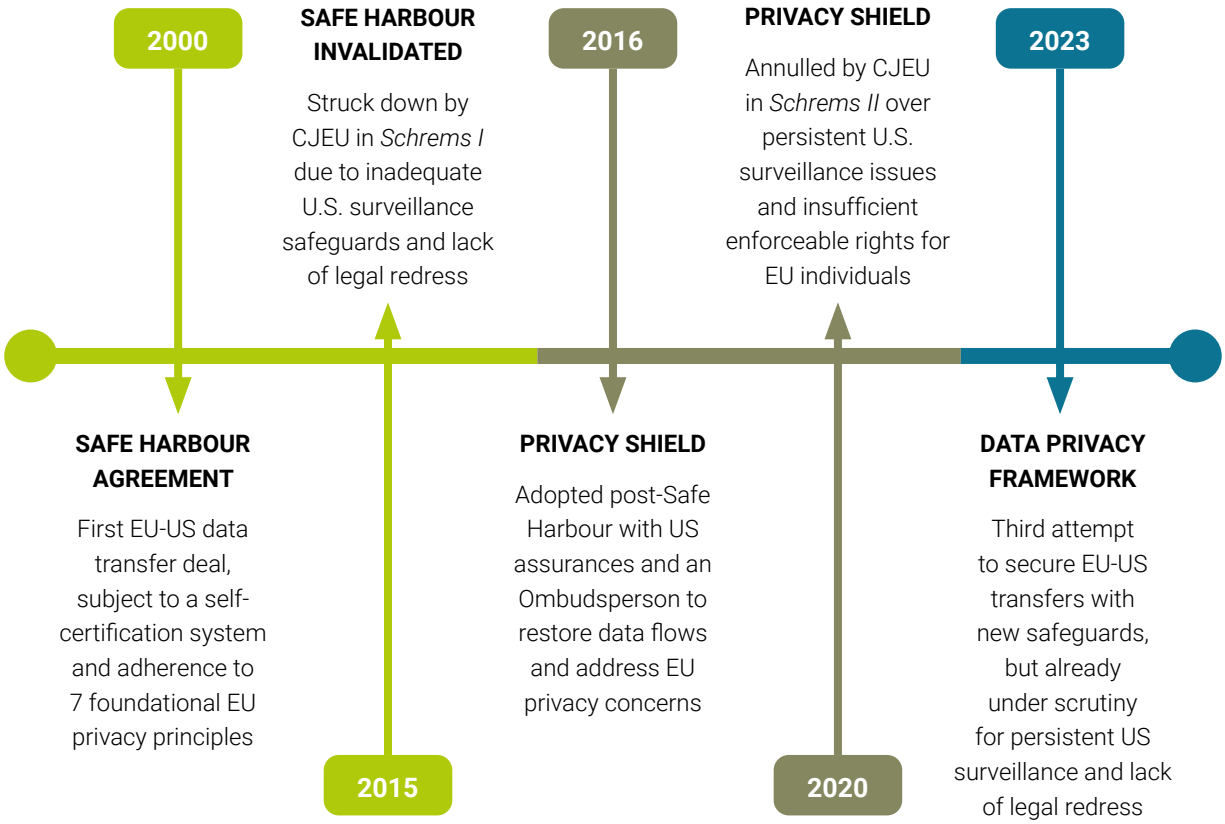
14 Schrems II, para 18

15 Schrems II, para 115

16 Schrems II, para 168

17 Schrems II, para 181

The DPF attempts to address some of these issues, particularly through Executive Order 14086, the creation of the Data Protection Review Court (DPRC), and enhanced oversight mechanisms, such as the Privacy and Civil Liberties Oversight Board (PCLOB). However, many of the structural weaknesses highlighted by the CJEU in *Schrems I & II* remain and may once again place the framework in legal jeopardy.



3. Does the DPF Offer "Essentially Equivalent" Protection?

In adopting the EU-US Data Privacy Framework (DPF), the European Commission, interestingly in contrast to the European Parliament,[18] concluded that recent US reforms, especially Executive Order 14086, now satisfy this standard. But a closer examination, combined with recent political developments, raises significant doubts concerning the framework's legal durability and institutional reliability.

3.1 What the US Legal Order Introduces

Executive Order 14086, signed in October 2022, forms the legal backbone of the DPF. It introduces safeguards intended to address the CJEU's concerns in Schrems II by requiring that signals intelligence be necessary and proportionate, a standard prominent in CJEU case law,[19] and by establishing a two-tier redress mechanism involving the Civil Liberties Protection Officer (CLPO) and a newly created Data Protection Review Court (DPRC). The DPRC is granted binding authority over US intelligence agencies, with access to relevant classified data, and US agencies are required to comply with its decisions. These measures aim to strengthen oversight and provide redress for EU individuals.

3.2 Why the DPF Still Falls Short

Despite these improvements, the DPF's structure and legal basis reveal several critical weaknesses, many of which mirror the concerns that invalidated its two predecessors:

- **EO 14086 Lacks Legal Stability:** It is a presidential directive, not a legislative act, meaning it can be changed or revoked at any time.
- **Bulk Surveillance Still Allowed:** EO 14086 permits bulk data collection for broad national security purposes (e.g. terrorism, cybersecurity),[20] and allows these objectives to be secretly expanded by the President.[21] While collection must be "as tailored as feasible,"[22] the vague language lacks the precision and proportionality required under EU law.
- **Redress Is Limited and Opaque:** The DPRC does not confirm whether surveillance occurred; complainants receive only generic responses.[23] It operates within the executive branch, with no appeals, public ruling, or access to evidence. Oversight by the PCLOB, key to its credibility, is also unstable, further weakening trust in the redress process.

18 European Parliament, 'Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework', B9-0234/2023

19 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others, 08.04.2014, ECLI:EU:C:2014:238; Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke and Hartmut Eifert v Land Hessen, 09.11.2012, ECLI:EU:C:2010:662; Schrems I

20 Executive Order No 14086, 'Enhancing Safeguards for United States Signals Intelligence Activities', 87 Fed Reg 62283 (Oct 7, 2022), §2(B)(i)A(1)-(12)

21 E.O. 14086, §2(b)(ii)(B), 2(c)(ii)(C)

22 E.O. 14086 § § 2(b)(ii)(B) & 2(c)(ii)(C)

23 E.O. 14086, § § 3(c)(i)(E)(1) & 3(d)(i)(H)

3.3 Oversight Breakdown: The PCLOB Crisis

In January 2025, the incoming Trump administration dismissed three Democratic members of the PCLOB, including its Chair. With only one member remaining, the Board lost quorum and became effectively non-functional. Given the historically slow and politicised appointment process no swift resolution is expected.

This collapse matters because the European Commission's adequacy decision explicitly relies on PCLOB oversight, including annual public reports.[24] Without a functioning PCLOB:

- There is no independent oversight of compliance with EO 14086.
- The DPRC's legitimacy is weakened, as the PCLOB was involved in vetting its fairness and appointing its members.
- The DPF's claim to provide an ongoing "essentially equivalent" protection is now in serious doubt.

In May 2025, a US federal judge ruled that the dismissal of two PCLOB members by President Trump was unlawful and ordered their reinstatement,[25] showcasing that key oversight bodies in the US remain politically vulnerable, raising serious doubts regarding the DPF's long-term validity.

24 Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU–US Data Privacy Framework [2023] OJ L231/118, Recital 110

25 Leblanc v United States Privacy and Civil Liberties Oversight Board, No 1:25-cv-00542 (D.D.C. 21 May 2025), ECF (No. 24)

4. Regulatory Warnings and the Growing of Schrems III

The EU-US DPF is legally fragile, and European regulators are increasingly treating it as such. National Data Protection Authorities (DPAs) have begun issuing formal warnings, calling for contingency planning, and, in some cases, enforcing the GDPR against unlawful US data transfers. These developments signal not only the growing likelihood of a Schrems III challenge, but a present and ongoing shift in enforcement posture, one that companies and organizations must address proactively.

4.1 Warnings from European Supervisory Authorities

Norway

The Norwegian Data Protection Authority warned that while the DPF is not formally dependent on the PCLOB, effective oversight and redress must work in practice, which currently, they do not. Norwegian authorities now advise businesses to:

- Remain vigilant and monitor legal developments.
- Prepare an "exit strategy" from the DPF.
- Be ready to switch to fallback mechanisms (e.g., SCCs).

EU Parliament

The Norwegian warning triggered formal political action at the EU level. On 5 March 2025, four MEPs submitted a priority written question (P-000941/2025) to the European Commission, inquiring whether:

The question challenges the Commission's adequacy decision following the reported dismissal of three PCLOB members by US President Donald Trump. Citing the Norwegian Authority's concerns, the MEPs asked:

- Whether the Commission will reassess the adequacy decision should the PCLOB remain non-functional.
- What contingency plans exist for businesses if the DPF is annulled.

This formal challenge signals growing institutional doubt at the EU level.

Denmark, Sweden, Finland

Denmark's Minister of Preparedness urged US tech companies to prepare for potential service disruptions in case the DPF is invalidated. Similarly, regulators in Sweden and Finland advised businesses not to view the DPF as a long-term solution, but instead to begin risk assessments and update fallback mechanisms such as SCCs and TIAs.

4.2 Enforcement Already Underway

Netherlands – Uber Case

On 22 July 2024, the Dutch Data Protection Authority (DPA) fined Uber €290 million for unlawful data transfers to the United States. The DPA found that Uber collected and retained sensitive personal data of European drivers, including account details, taxi licences, location data, photos, payment details, identity documents, and in some cases, criminal and medical data, on servers located in the U.S.

For over two years, Uber transferred these data to its U.S. headquarters without using appropriate transfer tools. After the Court of Justice of the European Union invalidated the Privacy Shield in 2020, Standard Contractual Clauses (SCCs) remained a valid transfer basis, but only if they could ensure an equivalent level of protection in practice. Uber stopped using SCCs in August 2021. According to the Dutch DPA, this meant the data were insufficiently protected. Since the end of 2023, Uber has relied on the successor to the Privacy Shield.

This case illustrates that relying on unstable frameworks can lead to non-compliance and significant costs, highlighting the importance of having a contingency plan in place should such frameworks fail.

France: Latombe Case

French MP and CNIL commissioner Philippe Latombe brought a legal challenge before the General Court of the CJEU (Case T-553/23), seeking to annul the DPF adequacy decision. On September 3, 2025 the General Court of the CJEU rejected this legal challenge and ruled in favour of the European Commission and thus upholding the Data Privacy Framework for EU-U.S. data transfers. Latombe may still appeal the General Court's ruling and the case signals the emergence of an imminent 'Schrems III'-like challenge that could once again overturn EU-U.S. data transfers.

5. What Happens if the DPF is invalidated – and What Should Businesses Do Now?

The EU-US Data Privacy Framework (DPF) was introduced to restore trust and legal certainty around sending personal data from the EU to the United States. But as we've seen that trust is quickly eroding. If the DPF is invalidated, either by a future court ruling (like a "Schrems III" case) or regulatory withdrawal, the impact will be immediate. Companies that rely on it to legally send personal data to the US could face operational disruption, legal consequences, and heavy administrative fines.

5.1 What Would Happen If the DPF Fails?

If the DPF is invalidated:

- Transfers of personal data to US companies relying solely on the DPF will become illegal overnight, similarly to *Schrems I & II*.
- Regulators can order data transfers to stop or issue fines, up to €20 million or 4% of global annual revenue.
- You'll need to switch quickly to another legal mechanism (like SCCs or BCRs when applicable), to maintain compliance.

5.2 What Should Businesses Be Doing Now

I. Map Transfers and Identify Vulnerabilities

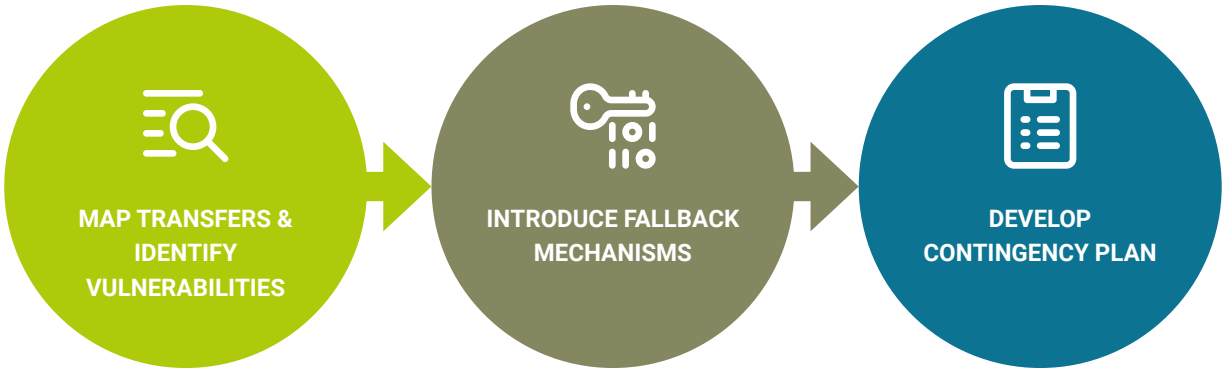
- Map all data transfers to the US that rely on the DPF, both internal (e.g. HR, finance) and external (e.g. vendors, partners).
- Identify which US entities are DPF-certified and whether alternative transfer mechanisms are already in place.
- Evaluate contracts, vendor agreements, and data flows to pinpoint high-risk dependencies.

II. Introduce Fallback Mechanisms

- For controlled transfers (e.g. intra-group), consider implementing springing SCCs that activate if the DPF is invalidated.
- Prepare supplementary safeguards (e.g. encryption) and TIA templates to support fallback mechanisms in compliance with Schrems II standards.
- Ensure documentation is in place and ready to activate with minimal delay.

III. Develop a Contingency Response Plan

- US companies: Create a prioritized list of EU clients relying on the DPF and draft SCC-based outreach plans.
- EU companies: List US data recipients and prepare SCCs + TIAs to deploy if needed.
- Communicate early with key partners and ensure internal teams are trained to respond quickly to regulatory disruption.



- Identify all DPF-based data transfers (internal & external).
- Check if US recipients are DPF-certified or use alternative safeguards.
- Review contracts and data flows for high-risk dependencies.

- Use springing SCCs for controlled (e.g., intra-group) transfers.
- Prepare encryption & TIA templates for fallback compliance.
- Ensure documentation is ready for rapid activation.

- US: List EU clients relying on DPF, prepare SCC-based outreach.
- EU: Identify US recipients, prepare SCCs & TIAs for quick deployment.
- Train teams and inform key partners proactively.

The EU-US Data Privacy Framework (DPF) was introduced to bring legal certainty to transatlantic data flows, but its long-term stability remains under serious doubt. The structural issues that led to the downfall of Safe Harbour and Privacy Shield, namely disproportionate surveillance, weak redress mechanisms, and political interference, persist under the DPF. Enforcement trends, political scrutiny from EU institutions, and emerging legal actions like the Latombe case suggest that a Schrems III ruling is on the horizon. As supervisory authorities begin signalling a shift away from treating the DPF as a reliable transfer mechanism, businesses must prepare for potential disruption. Mitigation depends on a proactive strategy grounded in risk awareness and legal resilience.

How We Can Help

In a landscape of legal uncertainty, we help you stay ahead. Our team supports you in identifying data transfer risks, conducting Transfer Impact Assessments (TIAs), and implementing robust legal mechanisms such as Standard Contractual Clauses (SCCs) or other GDPR-compliant tools under Chapter V. With our guidance, your business can ensure continuity, avoid disruption, and remain fully compliant, no matter what happens to the DPF.

Europalaan 28b
5232 BC 's-Hertogenbosch
The Netherlands

Congresstraat 35
1000 Brussels
Belgium

Office 5 Rec 2,
Retford Enterprise Centre,
Randall Way, Retford,
Nottinghamshire, England,
DN22 7GR

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com

DPO Consultancy
Experts in Data Privacy