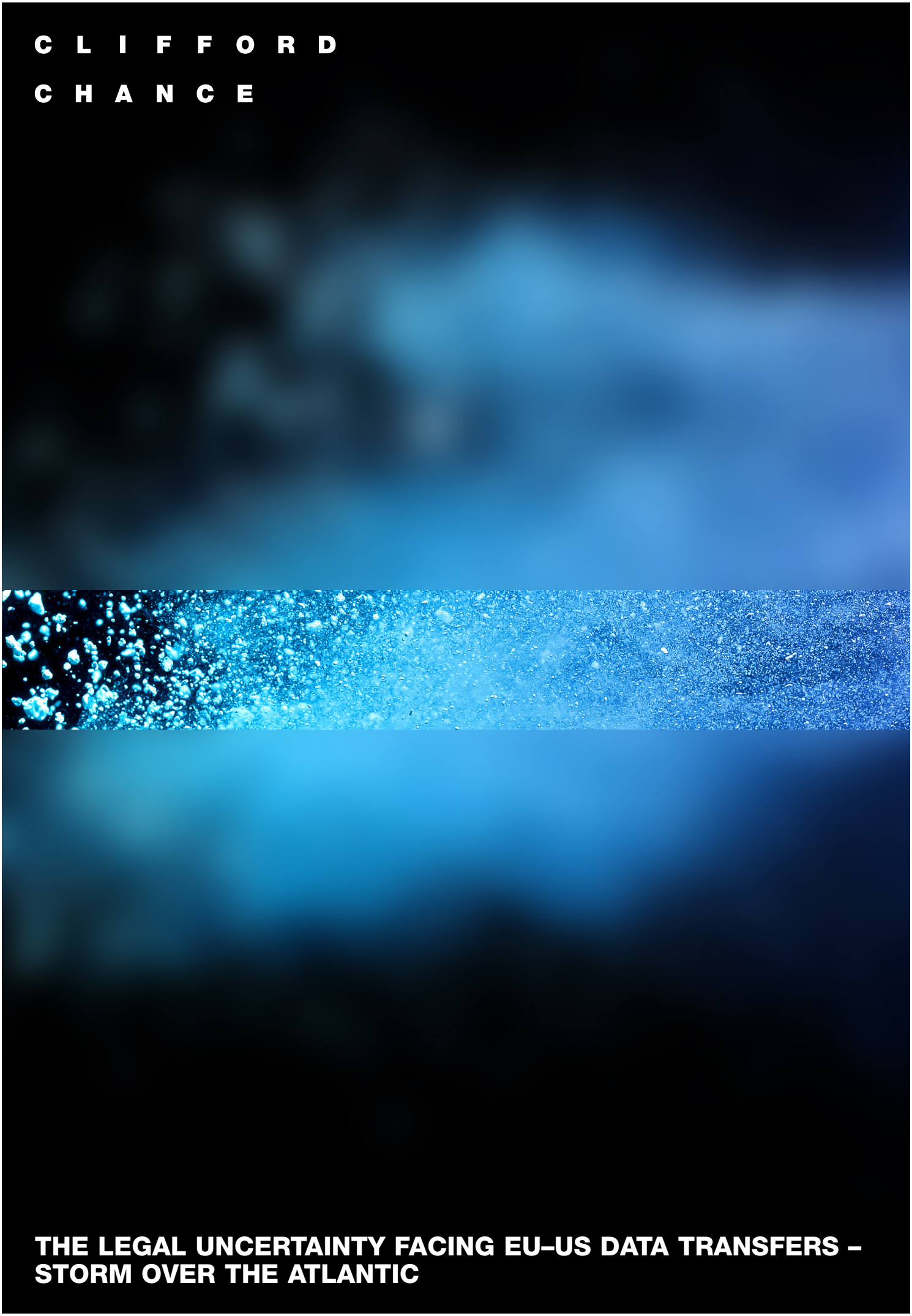
CLIFFORD

CHANCE



THE LEGAL UNCERTAINTY FACING EU–US DATA TRANSFERS – STORM OVER THE ATLANTIC

THE LEGAL UNCERTAINTY FACING EU–US DATA TRANSFERS – STORM OVER THE ATLANTIC

After a period of relative stability under the EU–US Data Privacy Framework (DPF), the climate has shifted: transatlantic data flows are once again under fire.

Despite the lack of demonstrable harm or concrete examples of misuse of EU citizens' data under the current EU–US DPF, critics continue to push for its annulment. The ongoing procedural challenge launched by French MP Philippe Latombe, and the recent political disruption, including the dismissal of Democratic members from the US Privacy and Civil Liberties Oversight Board (PCLOB), highlight an intertwining of litigation and geopolitics.

This dynamic is further compounded by reactions across the globe to new tariff measures introduced by the US, and by concerns raised by the US regarding the impact of the EU digital rulebook on US tech companies. In the EU, there is growing awareness of the role that digital regulation, including requirements around data governance, may play in broader strategic discussions.

Concerns are mounting over the prospect of repeated invalidations of EU–US personal data transfer mechanisms or the imposition of other restrictions which could impose additional burdens on businesses, fragment legal certainty and erode trust in carefully negotiated international instruments. This article discusses the DPF, the legal challenge to this framework and practical steps for organisations in a time of geopolitical flux.

1. The EU–US DPF: a refresher

On 10 July 2023, the European Commission finalised an eagerly awaited decision: it found that personal data transferred to organizations in the United States that are certified under the DPF did indeed enjoy a level of protection essentially equivalent to that in force in the EU (see our overview article **here**). With this green light (and an equivalent decision from the UK which followed later that year), Europeans' data would once again be able to circulate much more freely across the Atlantic. This procedure was made necessary by the successive invalidations of the two previous adequacy decisions: Safe Harbor, invalidated by the Court of Justice of the European Union in 2015 in the Schrems I ruling; and Privacy Shield, invalidated in 2020 in the Schrems II ruling.

The DPF was crafted with detailed safeguards and institutional oversight aimed at addressing the concerns raised in those decisions regarding US intelligence practices. Yet it now faces challenges which, if successful, could repeat the cycle of legal uncertainty.

- **From Schrems I to Schrems II: Judicial landmarks and cautionary tales**

  The rulings in Schrems I (2015) and Schrems II (2020) established the principle that EU personal data cannot be transferred to jurisdictions that do not offer protection that is 'essentially equivalent' to that in the EU unless additional safeguards are put in place that address relevant privacy risks. These cases exposed the inadequacies of Safe Harbor and Privacy Shield, particularly issues regarding redress for data subjects and oversight in US surveillance law. The CJEU's scrutiny in the Schrems cases resulted in clearer expectations: limitations on government access to data, remedies for EU citizens and increased transparency.

- **The DPF: structure and advancements**

  The DPF rests on Executive Order 14086 signed on 7 October 2022, which:

  - Imposes purpose limitations and proportionality standards on signals intelligence;
  - Establishes the Data Protection Review Court (DPRC) for complaints; and
  - Empowers the Civil Liberties Protection Officer within the intelligence community.

  The framework improves upon its predecessors by incorporating binding commitments, multilayer redress and real-time review by US oversight bodies. Importantly, it addresses many of the procedural and structural gaps noted by the CJEU in Schrems II.

  On 10 July 2023, the European Commission adopted an adequacy decision for the DPF, reflecting agreement by the European Commission that the DPF offers an adequate level of protection for personal data transferred from the EU to the US under Article 45 of the EU's General Data Protection Regulation (GDPR).

2. Latest developments: challenge before the EU General Court

At the 2025 InCyber Forum in Lille, Max Schrems stated that US surveillance laws still violate fundamental European rights, but also commented that he does not intend to initiate a third legal challenge. Instead, Schrems alluded to relying on the current US administration to unravel the DPF's credibility, citing recent removals of oversight officials and rollback of privacy mechanisms by President Trump, as reported by Politico in January 2025.

Meanwhile, French MP Philippe Latombe has initiated a direct challenge before the EU General Court, seeking annulment of the DPF adequacy decision; the first hearing took place on 1 April 2025. Although the MP's request for an emergency suspension of the DPF has been rejected, the main proceeding for annulment is ongoing. It is based on claims mirroring concerns raised in Schrems II and reflects concerns raised by the European Data Protection Board (EDPB) in its February 2023 opinion on the DPF (published prior to the adoption of the European Commission's adequacy decision relating to the DPF). These include concerns around the legality of bulk data collection and the effectiveness of redress mechanisms.

These criticisms echo long-standing tensions around US intelligence oversight, with EU bodies continuing to question whether executive-led reforms go far enough to guarantee fundamental rights. While the European Commission, balancing economic and legal imperatives, endorsed the DPF, the European Parliament and EDPB express principled scepticism. This divergence reflects a wider debate: should adequacy require theoretical perfection, or demonstrable protections and accountability?

While critics of the DPF argue that executive reforms do not fully cure previous deficiencies, proponents of the DPF point to the absence of demonstrated misuse of EU data as evidence supporting the framework's robustness. DPF supporters often draw on the argument that, to-date, no credible example has emerged of a disproportionate or unlawful US intelligence operation targeting or harming an EU citizen's data obtained under Safe Harbor, Privacy Shield or, now, the DPF. The debate therefore continues to reflect tensions between precautionary approaches and evidence-based assessments. With the DPF representing the outcome of sustained negotiation and structural reforms, it remains to be seen whether the European courts will ultimately align with the Commission's assessment or take a stricter view of equivalence, as well as what weight it will attach to the absence of identified real-world harms. There are fears that a decision based on a formalistic view may sacrifice hard-won protection for symbolic purity.

Joe Jones of the International Association of Privacy Professionals observed that Latombe's challenge may be the first to result in a substantive EU court ruling on the DPF's validity. Still, given potential appeals, a final decision may not materialize for another one to two years.

At present, however, the primary hurdle for Latombe's challenge before the EU court remains procedural: the admissibility of his direct action. Historically, such routes have been narrowly interpreted by the courts.

3. Wider political context

Although Latombe's original pleadings did not reference current US actions, developments such as the dismantling of oversight structures could bolster his case. In our **previous article**, we noted that the recent removal of Democratic members from the Privacy and Civil Liberties Oversight Board (PCLOB) has renewed European doubts about the independence and longevity of US privacy safeguards underpinning the DPF.

Beyond the courtroom, the debate over the DPF is increasingly shaped by wider geopolitical dynamics, as data transfers become entangled with broader questions of trade, sovereignty and strategic alignment in EU–US relations.

Recent developments in transatlantic trade relations have added complexity to the broader context in which the DPF is being assessed. New tariffs introduced by the US administration have contributed to a renewed strategic sensitivity between the US and the EU. Additionally, Members of the US Congress have raised concerns regarding the impacts of the EU digital rulebook on US firms and President Donald Trump recently issued a presidential memorandum indicating that the administration will take action with respect to tax and regulatory measures affecting US digital service providers. In Brussels and other EU capitals, there is a growing focus on the full range of instruments available to promote digital resilience, including the role of data transfers and localisation requirements.

In this evolving environment, data governance is increasingly viewed not only through a privacy lens but also as part of broader efforts to strengthen economic sovereignty and ensure regulatory consistency. Some policymakers have raised the question of whether frameworks like the DPF should be reassessed as part of a wider strategic dialogue between the EU and the US.

While no formal linkage has been established between trade measures and data governance, broader geopolitical developments may nevertheless influence the approach and timing of decisions relating to the DPF's future.

At the same time, the European Commission is considering easing a number of regulatory requirements in pursuit of competitiveness. In April 2025, Justice Commissioner Michael McGrath suggested that this could include revisiting long seen as untouchable provisions of the GDPR, such as those on data retention. In this vein, policymakers will doubtless be mindful of the detrimental economic impact of any invalidation of the DPF, not least to European digital competitiveness.

4. Business impact: real-world consequences of legal insecurity

The ongoing cycle of adequacy–adoption–legal challenge is destabilising for cross-border commerce, erodes trust in regulatory frameworks and can undermine lawful innovation.

The costs of such actions are not theoretical: thousands of businesses, particularly SMEs, depend on seamless data exchange with US service providers. The European Parliament's LIBE Committee, in its February 2023 resolution, also highlighted broader concerns over the fragility of international data transfer frameworks. Invalidation of the DPF would revive the compliance burden of Standard Contractual Clauses (SCCs) and Transfer Impact Assessments (TIAs) for many EU–US personal data transfers – and related questions as to what additional safeguards would be adequate. It may even

force some companies to exit the EU market or pursue data localisation, a costly and often technically unfeasible solution.

Proponents of the DPF argue that it represents a negotiated, enforceable and realistic response to long-standing concerns over transatlantic data transfers and, as such, should be evaluated not just against a doctrinal checklist, but on its ability to safeguard rights while enabling commerce in a globalized digital economy. The DPF's supporters argue that that there must be a serious, proportionate justification to suspend a framework that aligns surveillance oversight, judicial redress and corporate accountability in an unprecedented way. and that upholding the framework (unless and until real failures are demonstrated) reflects a pragmatic commitment to safeguarding both fundamental rights and economic resilience.

5. Practical steps for organizations

Given the uncertain and quickly evolving landscape, organizations should consider adopting a layered compliance strategy, including:

- Putting in place up-to-date SCCs as a parallel safeguard even for transfers made under the DPF;
- Considering the adoption of Binding Corporate Rules (BCRs), which offer a robust, long-term framework to govern intragroup transfers and may also be leveraged to legitimise some processor to sub-processor data flows under unified surveillance risks;
- Conducting and documenting Schrems II-compliant TIAs for US-bound data flows;
- Implementing technical and organizational safeguards such as encryption, data minimization and access controls to mitigate surveillance risks.

These measures not only reduce exposure should the DPF be invalidated but can also help serve to demonstrate accountability under the GDPR.

AUTHORS

Patrice Navarro
Partner
Paris
T: +33 1 4405 5371
E: patrice.navarro@cliffordchance.com

Egide Mugande
Stagiaire EFB
Paris
T: +33 1 4405 5982
E: egide.mugande@cliffordchance.com

Rita Flakoll
Global Head of Tech Group Knowledge
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

JOB0000066637