EU-US DP Framework: Progress, action items, and lingering questions

Nicholas Shepherd and **Daniel Cooper** of Covington assess the success of this framework which in the EU's view needs more active monitoring and enforcement.

On 10 July 2023, the European Commission (Commission) issued a decision finding that US law provides an adequate level of protection for personal data transferred from the EU to the US if the recipient organization is certified under the EU-US Data Privacy Framework (DPF).[1] One year later, in July 2024, the Commission conducted its first review of that adequacy decision and published its findings in a final report on 9 October 2024.[2]

The report concluded that the US has put in place sufficient structures and procedures to ensure the DPF functions effectively. It applauded the efforts of the US and EU to that end, noting progress on a number of fronts. The report also identified several action items for EU and US officials to focus on in the days ahead, including in relation to oversight and enforcement, awareness-raising activities, and certain topics requiring further guidance.

The Commission decided that its next formal review of the DPF will occur in three years. This is significant because the review cadence could have remained at one year if the Commission had material concerns about DPF's implementation, suggesting that it is headed in the right direction.

This article: (1) provides a short background on the DPF; (2) summarizes the progress mentioned in the Commission's report on the implementation of the DPF; (3) highlights action items that the Commission says EU and US officials should focus on going forward; and (4) considers a few lingering questions about the DPF, including how certain obligations apply to processors and how it may fare under the next US presidency.

Background on the EU-US DPF

The EU GDPR and similar laws in the UK and Switzerland permit transfers of personal data to non-EU/UK/Swiss countries which provide an adequate level of data protection comparable to the GDPR.[3] Absent an adequacy decision, organizations intending to transfer personal data from these jurisdictions to other "third countries" often must fulfill additional (and burdensome) requirements. These may include, for example, entering into Standard Contractual Clauses, obtaining Binding Corporate Rules certification, and fulfilling a range of related obligations.[4]

Thus far, the EU has recognized only 15 jurisdictions worldwide that provide an adequate level of data protection.[5] Adequacy decisions generally take one of two forms: (1) full adequacy, where the jurisdiction's legal framework as a whole is determined to adequately protect personal data; or (2) partial adequacy, where part of the recipient jurisdiction's legal framework provides adequate data protection, and organizations subject to that part of the framework may benefit from the adequacy determination.[6]

The DPF falls under the latter category, as it applies only to organizations in the US which join the DPF and meet its conditions (e.g., certifying compliance with the DPF Principles on an annual basis; revising privacy notices to include DPF-related disclosures; ensuring an independent redress mechanism is in place; identifying a contact person at the organization who is responsible for overseeing DPF compliance; paying all required fees; and so forth).

As readers will be aware, the DPF is the third transfer framework of its kind between the US and EU. Prior to the DPF, the Safe Harbor program existed from 2000 until 2015, while its successor, the Privacy Shield, was in effect from 2016 to 2020. Both of these frameworks were struck down by the Court of Justice of the European Union (CJEU) for not providing sufficient protections for EU personal data transferred to the US.[7] The CJEU's concerns focused, in particular, on the US government's broad data collection capabilities and practices for intelligence and national security purposes, and a lack of effective redress for EU residents impacted by these practices.

In October 2022, President Biden issued Executive Order 14086 (EO 14086) to address the CJEU's concerns, establishing privacy and civil liberties safeguards for US signals intelligence activities and creating a new form of redress for non-US persons.[8] EO 14086 and other steps taken by the Biden Administration enabled the EU and US to once again bridge the gap between their divergent privacy regimes. This led to the development of the DPF (and its "extensions" for UK- and Swiss-originating personal data), and the EU's adequacy decision in July 2023, all of which set the stage for the Commission's review a year later.

> The Department of Commerce, Federal Trade Commission, and Department of Transportation all confirmed that thus far they have not received any referrals or complaints.

Early signs of progress

In its report on the DPF at the one-year mark, the Commission cited several positive developments.

First, on the process of certification, the Commission noted that over 2,800 US organizations have joined the DPF so far, a faster rate of uptake than under the Privacy Shield.[9] The Commission

also highlighted the resources in place at the US Department of Commerce (DoC) to fulfill duties ranging such as facilitating timely DPF certification, rejecting applications that do not meet DPF requirements (which the DoC has done more than 30 times so far), and sending automated reminders to organizations ahead of their annual re-certification.

Second, in terms of practical implementation, DPF-certified organizations confirmed they have taken steps to adhere to DPF Principles such as access, choice, and onward transfer – including through updates to internal policies and procedures, revisions to contractual terms, adjustments to personal data rights procedures and channels, updates to employee training, and so forth.

Third, the Commission cited several developments in US laws and practices in the past year relevant to privacy. For example, it mentioned the ongoing proliferation of comprehensive state privacy laws across the US, and as well as executive orders issued on topics such as data transfers and artificial intelligence. The Commission also underscored that US intelligence agencies have adopted further policies and procedures to operationalize the changes set out in EO 14086. For example, FBI personnel must now be trained annually on rules that apply to the querying of information for intelligence purposes, and they are subject to further restrictions on the use of such data.[10]

Focus areas going forward

While the Commission struck an overall positive tone on the progress of the DPF, it also said that there remains plenty of work to be done.

In particular, in the area of complaints, the DoC, Federal Trade Commission, and Department of Transportation all confirmed that thus far they have not received any referrals or complaints of DPF non-compliance.[11] Similarly, the independent recourse mechanisms used by some of the DPF-certified organizations (e.g., BBB, VeraSafe, and others) reported receiving very few eligible complaints (which were swiftly resolved), while the panel made up of EU supervisory authorities has yet to hear a case. Further, the new redress mechanism that includes the possibility of appealing to the Data Protection Review Court (DPRC) has yet to receive any qualifying complaints from European residents.

While the Commission recognized that the DoC had to focus its resources in the first year on setting up the DPF, going forward, it expects more active monitoring and enforcement. It also attributed the lack of complaints so far to a gap in awareness among Europeans about their rights under the DPF and how to exercise them. Accordingly, it encouraged EU supervisory authorities to raise awareness by, for example, publishing more information on their websites about the DPF. The Commission also called on EU supervisory authorities to work with their US counterparts on guidance regarding certain DPF obligations, such the scope of "HR data" and how a cloud provider handling such data should address certain requirements.

Lingering questions

There are other parts of the DPF that also remain unclear, and where more guidance would be useful.

For example, the DPF does not frame its requirements according to the controller/processor concepts in the GDPR – rather, it simply sets out the DPF Principles and certification steps. This creates ambiguity around principles such as "Accountability for Onward Transfers," which requires DPF-certified parties to impose certain contractual terms on downstream recipients of the transferred data. This is relatively straightforward for a controller to do, but a DPF-certified processor must still act only at the instructions of the controller. Thus, a processor adding DPF contractual terms to the obligations it flows down from the controller is questionable in practice, and potentially at odds with its role. The EDPB has flagged this issue in its opinions on the prior Privacy Shield and the new DPF and called for clarification to avoid ongoing confusion and ensure that the DPF Principles are framed appropriately for processors to be able to rely on it.[12]

Lastly, one question that looms over the DPF is how it will fare in the next US presidency. To be clear, the saga of EU-US data transfers is now in its third decade and has seen four US presidents come and go. It has presented challenges for both Democrat and Republican administrations, and will likely continue to do so because, among other reasons, America's national security interests do not always fit squarely with European privacy norms. That said, a second Trump Administration is likely to strain US-EU relations once again, and could be harmful to the long-term viability of the DPF – although exactly how this would play out is unclear. On the one hand, the Biden Administration championed the DPF as a business-first solution to support US companies, which is broadly consistent with Trump's America-first policies, so his administration may not want to actively undo it. On the other hand, Trump may be inclined to pare back some of the restrictions placed on US intelligence agencies, which could give fuel to another legal challenge and/or ad-hoc review of the DPF by the Commission.[13]

Whatever ups or downs the next few years hold in store for EU-US data transfers, for now the DPF journey can be summed up in four words: so far, so good.

AUTHORS

Nicholas Shepherd is an Associate in Covington's US office in Washington, DC, and Daniel Cooper is the Co-chair of Covington's Data Privacy and Cyber Security Practice.
Emails: nshepherd@cov.com
dcooper@cov.com

REFERENCES

1 See 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 commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

REFERENCES

2 See Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework ec.europa.eu/info/law/better-regulation/

3 See Chapter V of the GDPR.

4 Article 49 of the GDPR also identifies derogations from the GDPR's cross-border transfer rules that organizations may rely on in certain limited scenarios.

5 European Commission, "Adequacy decisions." commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

6 For example, Canada's adequacy decision applies only to commercial organizations in Canada that are subject to the Personal Information Protection and Electronic Documents Act (PIPEDA).

7 See Case C-362/14, *Maximillian Schrems v Data Protection Commissioner,* 6 October 2015 (*Schrems I*) curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=6715724 ; and Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Ltd.*, 16 July 2020 (Schrems II) curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=en , respectively.

8 See Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities, October 7, 2022 www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ .

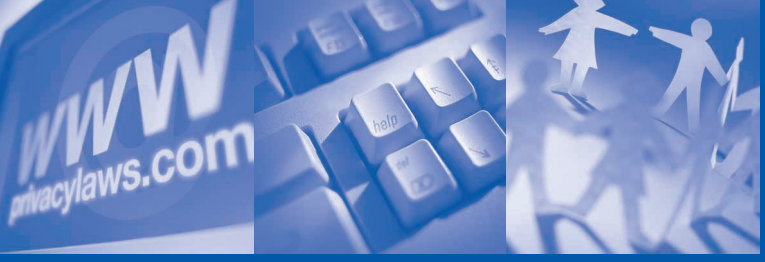
9 This number has grown to over 3,000 organizations at the time of this publication; see DPF Program List at www.dataprivacyframework.gov/list

10 See Reforming Intelligence and Securing America Act ("RISAA"), §§ 2(d) and 3(a) www.congress.gov/bill/118th-congress/house-bill/7888/text

11 The FTC did note that it now systematically checks for DPF violations as part of any privacy investigation it conducts, and several DPF-certified companies are currently under investigation.

12 See Opinion 01/2016 at Section 2.1.2 ec.europa.eu/newsroom/article29/items/640157 and Opinion 5/2023 at para. 41 www.edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf .

13 A French Member of the European Parliament (MEP) challenged the DPF in September 2023; while the CJEU rejected his attempt to halt the DPF as an interim measure, it has allowed the case to proceed. See Case T-553/23 R eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202301164



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

The Digital Markets Act – data portability re-booted?

Claudia Berg and **Tom Reynolds** of the UK Information Commissioner's Office[1] argue that data portability is enhanced by the EU Digital Markets Act, and explore its interactions with the GDPR.

Given the critical role of data in the digital economy, data portability is often mentioned as part of a digital competition policy reform agenda. Recently, it has gained traction under Regulation (EU) 2022/1925[2], commonly referred to as the Digital Markets Act (DMA). Data portability is not a new concept, however, and many will be familiar with the data portability rights granted to individuals under Article

Continued on p.3

Chile enacts new Data Protection Law

The new law, inspired by the GDPR, establishes a Data Protection Authority. **Natalia Jara Fuentealba** of Data Driven Legal explains.

After several unsuccessful attempts to amend Chile's current Law No. 19.628, entitled "Protection of Private Life" (the Data Protection Law), Congress and the Constitutional Court have approved the consolidated text of Bill No. 11144-07, merged with Bill No. 11092-07 (the Bill). The Bill was approved by the Constitutional Court on 14 November and will soon be published in the Official Gazette.

Continued on p.5

Issue 192 **DECEMBER 2024**

INTERNATIONAL report

ISSUE NO 192 DECEMBER 2024

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Natalia Jara Fuentealba
Data Driven Legal, UK

Claudia Berg and Tom Reynolds
Information Commissioner's Office, UK

Marc Schlegel
Federal Data Protection Authority, Germany

Katharina A. Weimer and Celin Fischer
Fieldfisher, Germany

Lars Lensdorf, Moritz Hüsch and Evangelos Karalias
Covington & Burling, Germany

Amit Ashkenazi
Law and Technology Expert, Israel

Graham Greenleaf
Independent Scholar, Australia

Abigail Dubiniecki
Independent Consultant, Canada

Nicholas Shepherd and Daniel Cooper
Covington & Burling, US and Belgium

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Data protection is a constantly evolving concept

When attending the Global Privacy Assembly (GPA) in Jersey this October (p.8), it was evident that while data protection principles are widely recognised, the Data Privacy Authorities' priorities differ depending on their jurisdiction's privacy maturity. For example, we heard that in Africa, 65% of the jurisdictions now have a DP law, but enforcement often needs to be stepped up. AI is of increasing importance but so are mobile payments, for example, and the privacy issues they bring.

In the EU, DPAs are still grappling with interpretations of the GDPR, and now also the interaction with the new EU digital legislation, such as the Digital Markets Act (see p.1). In Germany, there is some new case law that tries to clarify enforcement requirements and competition claims (see p.20).

Next year, the GPA goes to South Korea. It will be interesting to see which topics will be chosen – we have seen many new privacy laws emerge from the region in the last few years. This edition includes an analysis of Vietnam's new draft law which could be in force in 2026 (p.22), and Chile's new law which is about to be published in the Official Gazette (p.1).

As we start preparing for our own International Conference in Cambridge (7-9 July 2025), we are paying attention to the concept of human-centric data protection. After all, the laws are there to protect individuals who need to understand what rights they have and how to use them. Clear communication from DPAs and organisations is a key component. Nowhere is this needed more than in the field of AI as most people struggle to understand how their data is being used behind the scenes. Fulfilling the right to be forgotten in AI chatbots is easier said than done (p.29).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked in advance of the free-place deadline. Excludes the Annual Conference. More than one place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

> "Given the rate of change in law, regulation and business practice, it is essential to have concise and up to date information. *PL&B* is always relevant and continues to offer great value."
>
> **Adam Green, Chief Risk Officer, Equiniti**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the UK GDPR and related regulatory changes, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.