Third Time's a Charm?

Adequacy for the EU-US Data Privacy Framework

As announced[1] by the European Commission (EC), the new EU-US Data Privacy Framework (DPF) has been deemed adequate and entered into force on July 10, 2023. The DPF can now be used as a lawful transfer mechanism for controllers or processors in the European Economic Area (EEA) to transfer personal data to certified organizations in the US.

What does this mean for US organizations?

1. Personal data can freely flow from the EEA to DPF-certified US organizations. – Where EEA organizations had stopped transferring personal data to the US or put future projects on pause, the DPF provides the legal grounds for these transfers to occur.
2. Self-certification is still a requirement. – The adequacy decision[2] from the EC is only applicable to "certified organizations in the US." The Department of Commerce (DoC) will continue its administration duties. Per the DoC, companies that remained Privacy Shield certified must comply with the DPF Principles, including by updating privacy policies no later than October 10 2023, but will not need to make a separate, "initial" certification specific to the DPF[3].

What should US organizations remain aware of?

While this decision is welcome news for many on both sides of the pond, the legal challenges are expected to continue. NOYB and Max Schrems have commented[4] that they "have various options for a challenge already in the drawer" and expect the Court of Justice of the European Union will once again need to rule on whether the DPF truly provides an adequate level of protection.

In July 2024, the EC will conduct its first official review of the DPF to recertify that all elements of the Framework and corresponding measures have been successfully implemented to the satisfaction of the EC.

With a challenge on the horizon, US organizations planning to rely on the DPF should maintain a risk-based approach to cross-border data transfers, as outlined in the European Data Protection Board's

---

[1] Source: European Commission; *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows;* July 10 2023.

[2] Source: European Commission; *Commission Implementing Decision 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;* July 10 2023.

[3] Source: Data Privacy Framework Program; *FAQs - EU-U.S. Data Privacy Framework (EU-U.S. DPF);* 17 July 2023.

[4] Source: noyb; *European Commission gives EU-US data transfers a third round at CJEU;* July 10 2023

2021 guidance, and remember that previous rulings, including the recent Irish Data Protection Commission decision on Meta's case, had retroactive applicability.

US organizations that participate in EU-US cross-border data transfers should consider the following:

- Consulting with legal, risk, and privacy advisers to understand the impacts of the various transfer mechanisms on your organization
- If leveraging the DPF as the lawful mechanism for cross-border transfers is right for you as opposed to using other EU-approved transfer mechanisms (e.g., Standard Contractual Clauses, and Binding Corporate Rules)
- If you are seeking to self-certify under the DPF, begin preparation to update organizational privacy policies, notices, and practices to align with the requirements of the DPF, in addition to applicable privacy obligations.

How can KPMG help?

The KPMG Data Privacy & Protection practice offers several services that can help support an organization's preparedness for self-certification to the DPF and complying with the General Data Protection Regulation (GDPR), including, but not limited to, the following:

1. Review of data inventories (e.g., Records of Processing Activities), policies, and procedures related to cross-border data transfers and identify associated risks
2. Assess current data privacy and protection operations
3. Analyze control measures in place and conduct a gap assessment against applicable privacy requirements (e.g., the DPF and the GDPR)
4. Recommend and execute a roadmap to support alignment with the DPF's expectations.

Feel free to reach out to us for any questions or to further discuss how the decision impacts your organization.

Contact us

Orson Lucas
Principal
Cyber Security Services
E: olucas@kpmg.com

Stephen Bartel
Director
Cyber Security Services
E: sbartel@kpmg.com

Austyn McLoughlin
Managing Director
Cyber Security Services
E: austynmcloughlin@kpmg.com

Rachael Reinis
Manager
Cyber Security Services
E: rreinis@kpmg.com

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.