INSIGHT | October 12, 2023

Building Data Bridges and Bridging Legal Gaps: A New Era of Data Transfer Across the UK-US Data Bridge

Executive Summary

Today, the bridge officially opens! The UK-US Data Bridge ("Data Bridge"), that is, which is the UK extension to the EU-US Data Privacy Framework ("EU-US DPF"), providing a much-needed, streamlined mechanism for the lawful transfer of personal data between the UK and the US.

The Data Bridge is a positive development for businesses engaged in transatlantic data transfers. It simplifies the process of transferring personal data subject to the UK General Data Protection Regulation ("UK GDPR") to US organizations that participate in the Data Bridge, and eliminates the need for such companies to implement further, and often cumbersome, data protection safeguards such as International Data Transfer Agreements ("IDTAs") or binding corporate rules.

UK organizations are also exempt from conducting Data Transfer Impact Assessments (DTIAs) for US-bound data under the Data Bridge, removing an otherwise challenging and costly requirement.

Despite the Data Bridge's auspicious opening, however, businesses should exercise caution, consider maintaining alternative data transfer mechanisms, and stay updated on any legal developments that may affect the EU-US DPF's viability, and potentially send the Data Bridge falling down.

Background

The need for a robust and legally sound data transfer mechanism between the EU and the US has been a longstanding concern in the realm of data protection. Following the Court of Justice of the European Union (CJEU)'s invalidation of the EU-US Privacy Shield Framework in July 2020 (the so-called "Schrems II" ruling), organizations were left in a state of uncertainty regarding the legality of data transfers to the US.

In response to the *Schrems II* ruling, the EU and the US embarked on an ambitious journey to establish a new framework that would ensure the lawful transfer of personal data while addressing the concerns raised by the CJEU. The result was the EU-US DPF (available here), introduced in July 2023. This framework laid the foundation for transatlantic data transfers subject to the European Union's General Data Protection Regulation ("EU GDPR"). Participants in the EU-US DPF are deemed to provide adequate data privacy protections for cross-border data transfers.

However, a critical question loomed for the UK: How could organizations continue to transfer personal data subject to both the EU GDPR and the UK GDPR to the US in a manner compliant with EU and UK data protection laws? The UK, having left the EU, needed its own solution to bridge the data transfer gap.

The Data Bridge is the UK's answer to that challenge. It was officially established by the UK government on September 21, 2023, allowing businesses to commence operations under its provisions starting from October 12, 2023. This extension to the EU-US DPF (available here) provides a new legal avenue for the transfer of personal data from the UK to the US.

Key Objectives and Mechanisms

The primary objective of the Data Bridge is to ensure the lawful and secure transfer of personal data between the UK and the US, aligning with the principles of data protection and privacy. To achieve this, the Data Bridge relies on several fundamental mechanisms:

- **Participation in the EU-US Data Privacy Framework**: One of the critical requirements for US organizations to benefit from the Data Bridge is their participation in the EU-US DPF. To participate, eligible US companies must publicly confirm they will adhere to the EU-US DPF Principles and Supplemental Principles (collectively, "the Principles," found here); publicly disclose their privacy policies; and fully implement them. The Principles include a detailed set of requirements on how to protect and process personal data received from the EU, based on privacy considerations such as notice, choice, accountability for onward transfer, security, data integrity, purpose limitation, and access. The Principles also lay out access and recourse mechanisms that participants must provide to EU and, as applicable, UK individuals.

- **Data Bridge Participation**: US organizations can choose to participate in the Data Bridge during their annual self-certification to the US Department of Commerce confirming they agree to adhere to the Principles. Alternatively, US organizations can opt for participation outside of the annual recertification, provided they make this election within six months from July 17, 2023.

- **Data Privacy Framework List**: Organizations that have successfully elected to participate in the Data Bridge are listed on the Data Privacy Framework List. This list of US entities who have self-certified under the EU-US DPF and signed up to the "Extension" (that is, the Data Bridge) can be found here.

- **Eligibility**: Currently, only US companies subject to the jurisdiction of the US Federal Trade Commission (FTC) or the US Department of Treasury (DoT) are eligible to participate in the EU-US DPF program. US companies not subject to the jurisdiction of either the FTC or DoT — for example, banking, insurance, and telecommunications companies — are unable to participate in the EU-US DPF program at this time, and must continue to rely on pre-existing data transfer mechanisms, such as IDTAs or binding corporate rules.

Compliance Considerations

Compliance with the Data Bridge is paramount for organizations involved in transatlantic data transfers. Before crossing the Data Bridge, businesses on both sides of the pond should first undertake the following:

- **Verification of Participation**: UK-based businesses must verify whether their US partners are participating (or intend to participate) in the Data Bridge.

- **Privacy Policy Alignment**: Reviewing the privacy policies of US organizations is essential to confirm that they adhere to the Data Bridge's principles and standards. The privacy policy should align with the Principles.

- **Documentation Updates:** Both the transferor and transferee should update their privacy notices, records of processing, and contracts to reflect their reliance on the Data Bridge. These documents should accurately capture the data transfer mechanisms in place.

- **Handling Special Categories of Data**: Special category or sensitive data, criminal offense data, and data covered by the journalistic exemption require special attention. Additional steps or safeguards may be necessary to transfer such data in compliance with the Data Bridge. Journalistic data—that is, personal information that is gathered for publication, broadcast or other forms of public communication of journalistic material—cannot be transferred under the Data Bridge.

Legal Challenges and Uncertainty

The EU-US DPF has already encountered legal challenges due to concerns over the protection of EU citizens' personal data transferred to the US. These challenges may take quite some time to resolve, potentially up to 3 or 4 years.

The fate of the Data Bridge remains uncertain in the event that a challenge to the EU-US DPF is successful or the European Commission reverses its approval. Since it is an extension of the EU-US DPF, the Data Bridge's viability may be inexorably tied to the EU-US DPF's fate.

While the EU-US DPF's self-certification process simplifies data transfers, it's essential for organizations to consider maintaining alternative mechanisms—such as IDTAs or binding corporate rules—as fallback options. This ensures continuity in case of successful legal challenges or changes in the data transfer landscape.

Conclusion

The UK-US Data Bridge has emerged as a relatively smooth mechanism for facilitating transatlantic data transfers while adhering to data protection laws. It represents a significant step forward in resolving the challenges posed by the *Schrems II* ruling and provides a lawful basis for UK organizations to transfer personal data to the US.

Whether the Data Bridge will endure for the long term, or crumble down under the weight of legal attacks, remains to be seen. It is, therefore, essential for businesses to approach crossing the Data Bridge with care, ensuring compliance with its requirements and potentially exploring alternative routes for data transfers. The legal landscape surrounding data protection is complex and ever-evolving, making vigilance and adaptability key factors in navigating the intricacies of transatlantic data transfer.

If you have any questions about this article, please contact:

Robert McHale, Esq.
R | McHale Law
9 West Broadway, Suite 422
Boston, MA 02127
Tel. 617.306.2183
Email: robert.mchale@rmchale.com