Articles + Publications | December 7, 2023

U.S.-U.K. Data Transfer Developments

Privacy & Cybersecurity Newsletter

WRITTEN BY

Nick Elwell-Sutton

RELATED OFFICES

London

The U.K. Data Bridge extension to the EU-U.S. Data Privacy Framework ("DPF") was formally green-lighted by the U.K. Government on 12 October 2023.

The effect of this is that U.S. entities that have self-certified under the DPF in respect of data transferred from the EU can now extend the coverage utilizing the U.K. Data Bridge to permit the transfer of U.K. data and so will no longer be required to use other "appropriate safeguards", most commonly the ICO International Data Transfer Agreement, although it will remain a valid alternative.

The U.K. Data Bridge does not require a revocation of existing arrangements and they can run in parallel although in many cases this this may lead to an unnecessary "gold plating" of transfer protection.

Notably however, the U.K. Data Bridge cannot be applied for on its own and must be applied for as an extension to either a new or existing DPF certification.

The U.K. data regulator, the Information Commissioner ("ICO"), sounded a more guarded approach in two respects. First, that some U.K. GDPR protections are not replicated under DPF and, second, there is a marginal discrepancy between the protections afforded under the U.K. GDPR and the DPF in respect of certain sensitive categories of data: biometric data; genetic data; data concerning sexual orientation; and criminal offense data although in most cases these will only be relevant to a minority of data exporters.

These categories are not automatically treated as "sensitive" under the DPF and so will require U.K. entities exporting data to identify it as such to ensure it is treated as sensitive and with additional safeguards by the recipient organisation.

The areas not replicated, and where there are no equivalent DPF protections, are:

- The right to be forgotten;
- The right to unilaterally withdraw consent to processing; and
- Rights based on automated decision making.

The ICO did however note that while the DPF did have some safeguards in these areas, they were not as

extensive as the U.K. rights and it recommended that the Government reviewed the effectiveness in general every four years and on an ongoing basis in the areas of the operation of the DPF, the implementation and compliance with the requirements of Executive Order 14086 by the U.S. intelligence community, the effectiveness of U.S. oversight and enforcement bodies, and any significant changes in the U.S. legal landscape.

There is, however, a Schrems shaped cloud on the horizon. Privacy activist Max Schrems who managed to have the earlier Safe Harbor and Privacy Shield programs invalidated, has signalled his intention to challenge the EU decision that the DPF provides adequate safeguards. While any decision on this is probably 18 months to 2 years away, the continued uncertainty will be unwelcome to U.S. businesses and may act to discourage the uptake of DPF certification.

For more on the data transfer, see New Mechanism for Cross-Border Data Transfer: The EU-U.S. ?Data Privacy Framework.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber