DATA PROTECTION UPDATE

EU-US 'privacy shield' invalidated

In a judgment bringing the complexities of international data transfer back into focus, the Court of Justice of the European Union (CJEU) has invalidated the EU-US Privacy Shield. This briefing note recaps on the Privacy Shield and Standard Contractual Clauses, and summarises steps to take now.

Background

Under the General Data Protection Regulation ("GDPR"), "*appropriate safeguards*" must be in place for a controller lawfully to transfer personal data from within the EU to outside of it (Article 46).

- **SCCs**: One such safeguard is for the exporter and importer organisations to enter into European Commission-approved Standard Contractual Clauses ("SCCs").
- **EU-US Privacy Shield**: As an alternative safeguard specific to EU-US transfers, the Privacy Shield has been widely relied upon since its adoption in 2016 in the wake of the invalidation of its predecessor, Safe Harbor.

Key recent developments

In Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* ("Schrems II"), released on 16 July 2020, the CJEU found that SCCs are valid in principle, but the Privacy Shield is invalid.

The CJEU held that the Privacy Shield does not provide protection to EU data exported to the US which is "*essentially equivalent*" to the protections required under EU law.

It considered US laws relating to US authorities' access to EU personal data are not adequately safeguarded against by the Privacy Shield, nor do impacted data subjects have adequate redress in the US courts under the scheme.

SCCs contain real and challenging practical obligations on both exporters and importers. The CJEU clarified that transfers using SCCs require case-by-case assessment of the level of protection to personal data in the receiving country.

Steps to take now

The GDPR and its well-versed regulatory enforcement powers and data subject rights should be impetus enough for organisations to act swiftly, particularly given the CJEU judgment includes a specific call to action for supervisory authorities to intervene in invalid arrangements.

The UK government has confirmed it is working with the ICO to provide guidance to UK businesses, recognising the importance of maintaining the cross-border flow of data. As we await this guidance and any further guidance from the EDPB, organisations should begin considering and documenting their approach to identify any key risk areas.

Key steps to take now include:

- As a priority, identify any arrangements which rely on the Privacy Shield. Consider alternative safeguards you can implement to replace these, likely SCCs.
- Identify your arrangements which rely on SCCs. Think strategically about your organisation's processes for entering into (and complying with) SCCs and ensure data transfer is a key aspect of your data processing agreements going forward.

For **US-based suppliers**, tackling this issue head-on will be a key marketing tool in any engagement with EU customers. Appropriately considered contracts incorporating SCCs will put you in the best position to ease negotiation with those customers.

"Data localisation" (i.e. keeping data within the EU) will no doubt be considered by some, but a non-EU supplier hosting in the EU will not necessarily be the quick fix it might seem on the surface, nor does it fit as a desirable long-term solution given the inevitability of cross-border data flow in our globalised digital world.

Navigating international data transfer is set to remain a key data protection challenge in the coming years.

This note should not be treated as legal advice and only provides general information on the issues discussed.