BCLP. Client Intelligent

Insights

EU-US DATA TRANSFERS DEALT A SETBACK – PRIVACY SHIELD STRUCK DOWN BY EU'S HIGHEST COURT AND SCCS SUBJECT TO MORE SCRUTINY

Jul 16, 2020

Today's judgment by the Court of Justice of the European Union (CJEU) in the case known as "Schrems II" has far-reaching impact for businesses looking to ensure continuity of personal data flows between the EU and the US and other destinations.

The EU's data protection law – specifically the GDPR – restricts the export of personal data from the EU to countries which are not considered by the European Commission to have adequate data protection laws. There is a limited number of "gateways" through this restriction. The Privacy Shield program is – correction: *was* – one; the so-called "model clauses" or "SCCs" approved by the European Commission are another.

The court's sudden annulment of the European Commission's Privacy Shield Decision means that Privacy Shield is no longer valid as a legal mechanism for companies in the EU sending personal data to Privacy Shield program members in the US. At the same time, the court has confirmed that data transfers using SCCs may still be used. They are the most widely used transfer tool according to the European Commission.

The judgment also brings a sense of déjà vu. After all, it was only 5 years ago that a CJEU decision stemming from the same individual's complaint swept away the Privacy Shield's predecessor, "Safe Harbor".

This is a slightly unexpected twist in the legal tale which started in 2013 when Austrian privacy campaigner, Max Schrems, complained to the Irish Data Protection Commissioner that his Facebook data was being transferred from Ireland to the US unlawfully. The main focus of today's judgment was expected to be on the validity of the "model clauses" or SCCs and, no doubt to the relief of the business community, the SCCs remain a valid mechanism for transfers.

However, this is not an unqualified victory for SCCs - the judgment indicates that (a) companies entering into them may be expected to do more than merely signing up to them and (b) SCCs may be unsuitable (at worst) or vulnerable to challenge (at best) when relying on them to send data from

the EU to destinations operating bulk intelligence surveillance programs which extend to incoming personal data from the EU.

This poses some difficult dilemmas for businesses considering how best to respond to the CJEU's decision. We will be exploring this further during a webinar—additional details can be found here.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Kate Brimsted

Co-Author, London

kate.brimsted@bclplaw.com
+44 (0) 20 3400 3207