Katten

PRIVACY, DATA AND CYBERSECURITY ADVISORY

Privacy Shield Shattered: Standard Contractual Clauses Survive Glancing Blow

July 24, 2020

KEY POINTS

- The Court of Justice of the European Union (CJEU) struck down the EU-U.S. Privacy Shield (Privacy Shield) as a mechanism for transferring EU personal data to the United States;
- Standard Contractual Clauses (SCCs) remain a valid method to transfer personal data to processors established outside of the EU in most cases; and
- Organizations that previously relied on Privacy Shield must examine alternatives for lawful personal data transfers, such as SCCs or Binding Corporate Rules (BCRs).

On July 16, the European Union's top court, the Court of Justice of the European Union (CJEU) released its highly anticipated decision in the so-called *Schrems II* case,[1] which saw the EU-U.S. Privacy Shield (Privacy Shield) invalidated based on its failure to adequately address US government surveillance activities. As a result, companies that process personal data of EU persons in the United States are immediately faced with a new set of challenges for complying with the international personal data transfer requirements of the GDPR.

The European Union and the United States implemented the Privacy Shield framework in July 2016, after the CJEU scrapped the prior mechanism, the U.S.-EU Safe Harbor (Safe Harbor), in the 2015 *Schrems I* decision,[2] also because of surveillance concerns. Compared to Safe Harbor, Privacy Shield imposed stricter and more comprehensive data protection obligations on US organizations that handle personal data of EU persons. Since then, more than 5,000 companies have enrolled in Privacy Shield, which has been monitored and enforced by the U.S. Department of Commerce and the Federal Trade Commission.

While the CJEU upheld the use of Standard Contractual Clauses (SCCs), adopted and published by the European Commission or by a member state Supervisory Authority (SA), it emphasized that the contracting parties have an obligation to ensure that the laws in the recipient country are sufficient to protect EU personal data and cautioned that SAs are "required to suspend or prohibit the transfer of personal data to a third country," where the guarantees of the SCCs are not upheld.[3] The CJEU also noted that parties are encouraged to include additional safeguards beyond the SCCs themselves via supplemental contractual commitment.

[1] *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, case number C-311/18, in the Court of Justice of the European Union (July 16, 2020).

[2] *Maximillian Schrems v. Data Protection Commissioner*, case number C-362/14, in the Court of Justice of the European Union (Oct. 6, 2015).

[3] *Id.* at 14.

In the absence of Privacy Shield as a permitted mechanism for trans-Atlantic personal data transfers, there are important considerations for companies that transfer personal data to the US to ensure that they are continuing to process personal data of EU persons lawfully:

- Review the company's and its affiliates' personal data processing activities that involve international personal data transfers and identify which, if any, involve personal data transfers from the EU to the US;
- If any of these personal data transfers — whether between affiliates or third party service providers — have relied on Privacy Shield certification, put in place a new adequate personal data transfer mechanism: (1) SCCs, but noting that based on the CJEU decision that additional diligence, considerations and provisions may be advisable; or (2) with respect to internal corporate and affiliate transfers, Binding Corporate Rules (BCRs), which allow multinational companies to transfer personal data to other entities abroad within the same enterprise under the supervision of a SA that must approve their global privacy policies and procedures; and
- If SCCs or BCRs are not practical, determine whether it is feasible to obtain the consent of the personal data owners for the cross-border transfer.

Schrems II serves as an important reminder to assess (or re-assess) whether your privacy program has adequate safeguards in place to protect personal data of EU persons, which must be afforded "a level of protection essentially equivalent to that guaranteed within the EU by the GDPR."[4]

[10] *Id.* at 21.

CONTACTS

For more information on the international personal data transfer requirements, please contact Katten's Privacy, Data and Cybersecurity team or any of the following attorneys:

Christopher Hitchins
+44 (0) 20 7776 7663
Christopher.hitchins@katten.co.uk

Doron Goldstein
+1.212.940.8840
Doron.goldstein@katten.com

Nathaniel Lalone
+44 (0) 20 7776 7629
Nathaniel.lalone@katten.co.uk

Jeremy Merkel
+1.212.940.6339
Jeremy.merkel@katten.com

Sarah Simpson
+44 (0) 20 7770 5238
Sarah.simpson@katten.co.uk

Katten katten.com

CENTURY CITY | CHARLOTTE | CHICAGO | DALLAS | HOUSTON | LONDON | LOS ANGELES | NEW YORK | ORANGE COUNTY | SHANGHAI | WASHINGTON, DC

7/24/20