October 7, 2015

The Court of Justice of the European Union Sinks the Safe Harbor Program

The End of Safe Harbor

In a decision that could significantly impact those doing business in the United States and Europe, the European Union's highest court ruled on October 6, 2015, that the U.S.-E.U. Safe Harbor program[1], which allowed for trans-Atlantic data transfers between the United States and European Economic Area (EEA), is invalid effective immediately and without a transition period. The Safe Harbor program enabled companies to legally transfer data between the EEA and the United States in compliance with the European Data Protection Directive (the "Directive"), which generally prohibits transfer of personal data outside of the EEA. Currently, more than 4,000 companies are members of the now-defunct Safe Harbor program.

In this highly anticipated opinion, the Court of Justice of the European Union (CJEU) concluded that the Safe Harbor scheme that governs the transfer of personal data fails to adequately protect the privacy rights of EU citizens. In essence, the Safe Harbor program puts the rights of US law enforcement officials above the rights of EU citizens by allowing the US government unfettered access to the transferred EU personal data, according to the court. The CJEU also concluded that the European data protection authorities (DPAs) have the power (and responsibility) to investigate claims and suspend transfers of EU personal data that take place under the Safe Harbor arrangement, notwithstanding the European Commission's overall approval of the Safe Harbor program in 2000.[2]

As a result of this decision, companies relying on Safe Harbor registration to transfer EU personal data to the United States (or to receive that data from EU companies) will need to adopt alternative processes to comply with the Directive. Some of these alternative processes include DPA-approved model contracts and clauses, binding corporate rules, or use of the data owners' consent.

Maximillian Schrems v. Data Protection Commissioner, Case No. C-362/14

The case was brought by an Austrian national, Maximillian Schrems, who was a subscriber to Facebook. All Facebook subscribers residing in the EU are required to agree to a contract with Facebook Ireland, a subsidiary of the US-based parent

[1] *See* the U.S. Department of Commerce's International Trade Administration's overview, available here.

[2] *See* Commission Decision 2000/520, available here.

For more information, please contact any of the following members of Katten's **Privacy, Data and Cybersecurity** and **Technology** practices.

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Megan Hardiman
+1.312.902.5488
megan.hardiman@kattenlaw.com

Leonard A. Ferber
+1.312.902.5679
leonard.ferber@kattenlaw.com

Tanya L. Curtis
+1.312.902.5593
tanya.curtis@kattenlaw.com

Claudia Callaway
+1.202.625.3590
claudia.callaway@kattenlaw.com

company, Facebook, Inc. ("Facebook USA"). Some or all of the data of subscribers to Facebook Ireland is transferred to Facebook USA's servers in the United States, where it is stored.

Mr. Schrems' complaint—originally submitted to Ireland's Data Protection Commissioner in June 2013—claimed that the law and practices of the United States offer no real protection against governmental surveillance of the data stored in the United States. His claims were based on the revelations made by Edward Snowden from May 2013 concerning the activities of the US intelligence services, in particular those of the National Security Agency (NSA). According to those revelations, the NSA obtains unrestricted access to mass data stored on servers in the United States owned or controlled by a range of companies active in the Internet and technology field, such as Facebook USA.

The CJEU concluded that the US national security, public interest and law enforcement requirements will always prevail over the Safe Harbor program. As a result, the United States is "bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict . . . ."[3] Moreover, persons concerned have no administrative or judicial means of redress, which normally would allow the data relating to them to be accessed, rectified or erased.

The CJEU said that, in order for the interception of electronic communication or data by the US government to be permitted under the Directive, "it would be necessary to demonstrate that the interception is targeted, that the surveillance of certain persons or groups of persons is objectively justified in the interests of national security or the suppression of crime[,] and that there are appropriate and verifiable safeguards."[4] However, the recent collection of personal data demonstrated a significant over-reach on the part of the US government. As a result, the mass, undifferentiated access to personal data obtained from companies seemingly in compliance with the Safe Harbor runs afoul of the transparency and proportionality principles enshrined in the Directive.

The Future of EU-US Data Flows

The CJEU's ruling is definitive and cannot be appealed. Thus, it will have a significant impact on organizations with EU-US data flow. Certain DPAs have already issued statements addressing the CJEU's decision, recognizing the inherent tension left in its wake. For example, the UK Information Commissioner's Office released a statement today advising businesses that rely on the Safe Harbor program to review their existing practices to "ensure that data transferred to the [United States] is transferred in line with the law," while also recognizing that "it will take them some time for them to do this."[5] While statements from regulators like this provide some comfort, companies should remain vigilant of the risks of non-compliance, including fines and enforcement.

In the next few days, there likely will be a statement and guidance from the Article 29 Working Party—an EU advisory body comprised of representatives of the DPAs of all EU Member States, the European Data Protection Supervisor and the European Commission.

At the same time, pressure will mount on US and EU politicians to reach an agreement on an updated trans-Atlantic data transfer paradigm. The parties have been negotiating for more than two years, but there is no announcement on when they hope to finalize an update scheme.

---

[3] Press Release, *The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid*, No. 117/15, Court of Justice of the European Union (Oct. 6, 2015), available here.

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

[5] *ICO Response to ECJ Ruling on Personal Data to US Safe Harbor*, U.K. Information Commissioner's Office (Oct. 6, 2015), available here.

What This Means to You

Until a replacement, if any, is put in place by the United States and EEA, it is important to recognize that there are other viable alternatives to the Safe Harbor program. These options include DPA-approved model contracts and clauses, binding corporate rules (whereby multinational companies can have a DPA approve of their world-wide privacy procedures) and the use of the data owners' consent. These alternatives will likely pose large administrative undertakings and some, including the binding corporate rules, take time to implement. Determining the best alternative for a given company will depend on a number of factors, but those who have relied on the Safe Harbor until now should be actively looking into those.

In addition, this decision may require looking into existing vendor agreements, if any involve the potential of EEA-US data transfers, and imposes a potential new layer of complexity on transactional due diligence and even potentially on litigation discovery involving parties in the EEA.