KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

October 7, 2015

The Post-Safe Harbor Era Begins: What In-House Counsel Needs to Know

On October 6, 2015, in a landmark ruling by the European Court of Justice (ECJ) in *Maximillian Schrems v. Data Protection Commissioner* (C-362/14), the ECJ declared invalid the Safe Harbor framework that has streamlined the transfer of personal data from Europe to the United States since 2000. The decision makes it prudent for any company that relies on the Safe Harbor framework to reevaluate its data transfer programs and their legality.

The Safe Harbor framework was intended to ensure data stored in the United States regarding European citizens had the same privacy protections as it would when held in the European Union. In 2014, the Safe Harbor framework was challenged in Ireland by an Austrian privacy activist, Max Schrems, who was concerned about the impact of U.S. national-security surveillance as revealed by Edward Snowden's disclosures. Mr. Schrems alleged that Facebook was supporting U.S. spying by passing on its users' data to the government.

When Mr. Schrems brought his case before the Irish Data Protection Commissioner (where Facebook's European headquarters are based), the data protection authority dismissed his complaint, holding that it would not pursue the case in view of previous decisions declaring the Safe Harbor legitimate. Mr. Schrems appealed that decision to the High Court in Dublin, which referred the case to the ECJ.

In the decision at issue, the ECJ held that the Irish authority would need to examine Schrems' complaint "with all due diligence" to decide whether the transfer of personal data of Facebook's European users to the U.S. should be suspended.

The ECJ also held that protections for personal data in the United States are not as strong as those offered in the EU and, for essentially this reason, the Safe Harbor framework violated EU law. In this connection, the Court stated "the national security, public interest and law enforcement requirements of the United States prevail over the Safe Harbour scheme, so that United States undertakings are bound to disregard, without limitation,

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Jane Player
+44 20 7551 2130
jplayer@kslaw.com

Angela Hayes
+44 20 7551 2145
ahayes@kslaw.com

John A. Drennan
+1 202 626 9605
jdrennan@kslaw.com

Nicholas A. Oldham
+1 202 626 3740
noldham@kslaw.com

Sebastian D. Müller
+49 69 257 811 201
smueller@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

London
125 Old Broad Street
London EC2N 1AR
T: +44 20 7551 7500

the protective rules laid down by that scheme where they conflict with such requirements."

The ECJ's decision, which cannot be further appealed, came after Advocate-General Yves Bot advised the ECJ that the United States had carried out "indiscriminate surveillance" incompatible with EU fundamental rights.

What Should Clients That Transfer Personal Data From the EU to the United States Do Now?

The single most important thing for clients to do at this point to protect themselves from legal challenges is to contact experienced counsel and conduct thorough, independent assessments of their legal and operational protections for personal data both inside and outside of Europe.

While the ECJ decision will undoubtedly have significant and far-reaching consequences for U.S. businesses, clients must understand that there is no need for panic in the C-suite. As a practical matter, the decision's legal effect on the Safe Harbor program will not be felt immediately. The proceedings in Ireland that gave rise to the decision will continue, and although it is reasonable to expect activists to begin challenging other companies' privacy programs before various Data Protection Authorities, such challenges could take months to move through the judicial system. In theory, this could give U.S. authorities and the European Commission enough breathing room to negotiate a new Safe Harbor agreement that provides DPAs an enhanced opportunity to address complainants' privacy concerns. The UK Information Commissioner's press release in response to the ECJ judgment states: "The judgment means that businesses that use Safe Harbor will need to review how they ensure that data transferred to the US is transferred in line with the law. We recognize that it will take them some time for them to do this."

Equally important, EU Data Protection Directive 95/46/EC provides a measure of flexibility that can be used to the advantage of U.S. businesses. For example, as the ECJ opinion points out, the Directive sets out several "derogations" that permit the free flow of personal data from Europe to the United States. These include informed consent; transfers required for the performance of a contract between an individual and a business; transfers required to conclude or perform a contract between a business and a third party when the contract is in the interest of the individual and the business; transfers justified by important public interest grounds, or to exercise legal claims; and transfers that are required to protect the vital interests of the data subject.

Where one or more of these "derogations" apply, companies can work with their counsel to formulate and document their rationales for relying on them.

There are other possibilities. Businesses can use model clauses approved by the European Commission as an alternative to the Safe Harbor Program. While these clauses can be difficult to administer, for a business that does not have a complex structure and can effectively negotiate them with its partners, they are a viable means to satisfy European privacy requirements.

Binding Corporate Rules (BCRs) arguably provide a longer-term solution, especially for larger businesses that have contracts with partners across the globe. As is true of many governance-structuring solutions, BCRs can be time-consuming to implement, but they can save time and money over the long-run due to the relative ease of administration and the fact that BCRs provide a single solution for all global transfers from Europe, not just those to the United States.

Finally, many business will be able to use pseudonimization and anonymization techniques. While care must be exercised because some DPAs base the threshold of identifiability on whether "any party" can identify an individual from the data rather than the party in possession of the data, a U.S. business, say, that conducts employee surveys might consider anonymization to meet European requirements.

King & Spalding's Data, Privacy, and Security Practice

With more than 50 Data, Privacy & Security lawyers in offices across the United States, Europe, and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy and cybersecurity-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy. Our **Data, Privacy & Security Practice** has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents including data breaches and cybersecurity incidents, interfacing with stakeholders and the government, engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of state and federal government.

If you have any questions about the EU/US Safe Harbor, EU model clauses and Binding Corporate Rules (BCRs), or related issues, please contact **Phyllis B. Sumner** at +1 404 572 4799, **Jane Player** at +44 20 7551 2130, **Angela Hayes** at +44 20 7551 2145, **John A. Drennan** at +1 202 626 9605, **Nicholas A. Oldham** at +1 202 626 3740, or **Sebastian D. Müller** at +49 69 257 811 201.