KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

February 4, 2016

EU-U.S. Privacy Shield Framework Agreement Reached
Replaces Safe Harbor Agreement

On February 2, 2016, The European Commission (EC) and the U.S. Department of Commerce (Commerce) reached a deal on a new transatlantic data-transfer pact to replace the 15-year-old Safe Harbor agreement. The European Court of Justice invalidated the Safe Harbor agreement in late 2015 on the ground that it failed to adequately protect the privacy rights of EU citizens.

The text of the replacement agreement—dubbed the EU-U.S. Privacy Shield—has not yet been released, but the EC issued a Press Release about the agreement and several aspects of it are of immediate significance to companies involved in transnational transfers of personal data (*e.g.*, employee and consumer data). Two notable changes are:

- U.S. companies that import personal data from Europe will need to commit to robust obligations concerning how they process personal data and protect individual rights. The U.S. Department of Commerce will ensure that companies publish these commitments, making them enforceable by the Federal Trade Commission (FTC). In addition, any company handling human-resources data from Europe must comply with decisions by European Data Protection Authorities (DPA).
- New redress mechanisms will be available to individuals in the EU who believe they have been wronged by a U.S. company's collection, processing, transfer, or destruction of their personal data. Under the new pact, any citizen who believes that his or her data has been misused will be permitted to file a complaint with a DPA, and U.S. companies will have deadlines to respond to the complaint. Further, the DPA receiving the complaint will be able to refer the matter to the Department of Commerce and the FTC. Alternative dispute resolution may be used and will be free of charge.

In addition, new safeguards and transparency obligations will be imposed on the United States government regarding access to information from the EU. In announcing the agreement, Věra Jourová, an EC Commissioner, stated that "the U.S. will provide written assurances" from the White House Director of National Intelligence regarding limitations on access to data by law enforcement and national security agencies. The EU Press Release

For more information, contact:

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

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

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

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

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

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

Kim Roberts
+44 20 7551 2133
kroberts@kslaw.com

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

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521

London
125 Old Broad Street
London EC2N 1AR
United Kingdom

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707

www.kslaw.com

stated that the United States has ruled out indiscriminate mass surveillance of transferred EU personal data. The United States has also agreed to an annual joint review of the functioning of the arrangement, performed by the EC and the Department of Commerce. Additionally, a new Ombudsperson position will be created to address complaints based on alleged improper access to personal data by U.S. national security authorities.

The announcement comes at a time of significant upheaval in the EU's efforts to protect the data and personal information of EU citizens. In October 2015, the European Court of Justice declared invalid the Safe Harbor framework that had streamlined the transfer of personal data from Europe to the United States since 2000. Whether the new Privacy Shield Framework Agreement will suffer a similar fate is an open question. But continued concern in the EU about the privacy of personal data transferred to the United States is a distinct possibility, and may lead to skepticism about the new agreement. Further, in December 2015, the EU reached agreement on a new General Data Protection Regulation (GDPR) to replace the EU current data privacy directive (95/46/EC). The GDPR strengthens data protection law in the EU in a variety of ways, including by tightening the rules around data transfer and consent, and by dramatically increasing the penalties for violations of the law.

Recommendations

Companies engaged in transfers of personal data (broadly construed) from EU countries to the United States should contact counsel to determine their obligations and compliance options under the new pact. EU regulators must approve the agreement before it becomes effective, and it is not yet clear how they will receive it, leaving its status uncertain. The agreement was reportedly presented to EU privacy regulators on Wednesday, February 3, 2016, and the Article 29 Working Party, an independent advisory body to the European Commission, said during a press conference that the group "welcomed" the agreement but needed further documentation to assess its legality. The Working Party further indicated that if it receives the documentation by the end of February, it will meet to assess the agreement in March, and could come to a conclusion on whether the Privacy Shield is acceptable by mid-April or the end of April. King & Spalding will continue to update its clients as the details of the agreement become available.

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 60 Data, Privacy & Security lawyers in offices across the United States, Europe, Russia, 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 data security-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.