KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

March 7, 2016

EU-U.S. Privacy Shield Agreement Released

On February 29, 2016, the European Commission ("EC") and the U.S. Department of Commerce ("Commerce") released the long-awaited text of the European Union ("EU") – United States ("U.S.") Privacy Shield, an agreement-in-principle that, if approved by European authorities, would replace the Safe Harbor Framework as a potential basis for transatlantic transfers of personal data. The Safe Harbor Framework was invalidated by the European Court of Justice in October 2015, when the Court found the agreement failed to provide adequate protection for EU citizens' privacy rights.

The new agreement is presented as a 128-page "package," including the EU-U.S. Privacy Shield Framework Principles, an annex on the arbitral model, and numerous letters from U.S. officials. It notably ups companies' obligations and, although mimicking the self-regulatory structure of the Safe Harbor, it adds sharp enforcement teeth. Under the Privacy Shield, for example, companies will be required to resolve consumer complaints within 45 days and European data protection authorities ("DPA") can work with the U.S. Federal Trade Commission ("FTC") to ensure compliance. The enforcement staff at Commerce will be substantially increased, as well as the penalties for companies found to be out of compliance.

Corporate Commitments

Like the old Safe Harbor Framework, the Privacy Shield operates through a self-certification system. Companies wishing to make use of the Privacy Shield will be required to file with Commerce and re-certify annually. The companies commit to publishing their privacy policies and to providing links to them on Commerce's website. They must allow individuals to opt out of the use of information for direct marketing and third party disclosure, as well as establish consent before using sensitive private information for a purpose other than that established at the initial collection.

Companies must inform individuals of their right to access personal data, the options for dispute resolution, and the possibility of binding arbitration.

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

Christine E. Savage
+1 202 626 5541
csavage@kslaw.com

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

Joseph Laroski
+1 202 626 2647
jlaroski@kslaw.com

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

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

Kathleen L. Benner
+1 202 626 5403
kbenner@kslaw.com

www.kslaw.com

They are further required to take reasonable and appropriate steps to protect private information and to provide individuals access to their own information, including the rights to amend or delete.

Individuals are encouraged to raise complaints to companies, which must provide recourse mechanisms that are readily available and free of charge. Once a complaint is filed, the companies must respond within 45 days. If the disputed information is human-resources information, the companies need to comply with decisions made by a DPA. Unresolved complaints can be submitted by the individual or a DPA to Commerce, which must respond in 90 days. Cases can then be brought before the FTC. If other avenues fail, individuals can move to a binding arbitration panel, which is empowered to make decisions that are enforceable under the U.S. Federal Arbitration Act. Notably, individuals in the EU are permitted to pursue legal remedies through private causes of action in U.S. state courts, including private causes of action for misrepresentation and similar claims.

Commerce will take the lead in monitoring compliance with the Privacy Shield. Enforcement measures include verifying attestations through self-assessments signed by corporate officers or outside compliance reviews, the requirement to respond to requests for information from Commerce, and sanctions such as publicity of non-compliance, deletion of information, suspension, compensation for individuals wronged, and injunctive awards. Persistent failure to comply with the Privacy Shield will lead Commerce to remove a company from the list and the removed company will be required to delete or return the personal information acquired while under the Privacy Shield.

Government Commitments

The agreement also has implications for the use of private data by the U.S. Government. One new element of oversight is the establishment of the independent Privacy Shield Ombudsperson. The Senior Coordinator for International Information Technology Diplomacy, currently the U.S. State Department's Under Secretary of State for Economic Growth, Energy, and the Environment, a person outside of the U.S. intelligence community, serves in this role. The Ombudsperson will work with the EU individual complaint handling body to respond to complaints and address governmental non-compliance with intervention by federal Inspector Generals.

The EU's fact sheet claims that U.S. authorities "affirm absence of indiscriminate or mass surveillance." But a letter from the U.S. Office of the Director of National Intelligence that forms part of "package" suggests otherwise. The letter states that Presidential Policy Directive 28, which President Obama issued in January 2014, permits the U.S. intelligence community to "collect bulk signals intelligence in certain circumstances," including for detecting and countering certain activities of foreign powers, counterterrorism, counter-proliferation, cybersecurity, detecting and countering threats to U.S. or allied armed forces, and combating transnational criminal threats. With that said, the letter notes that Presidential Policy Directive 28 requires the U.S. intelligence community to prioritize alternatives that would allow targeted surveillance where possible. Finally, the letter states that access to private information will be subject to safeguards and oversight.

Next Steps

The Privacy Shield is still provisional. Prior to becoming law, a committee of representatives from the 28 EU Member States and the Article 29 Working Party of the European Parliament and Council, established under Data Protection Directive 95/46/EC, must conduct a detailed review of the Privacy Shield and conclude that the Privacy Shield offers

"adequate" protections to personal data.. After the review, if accepted, the European Commission's College of Commissioners can adopt a Final Adequacy Decision enabling personal data to move from the EU and European Economic Area (EEA) countries to the United States under the Privacy Shield.

Alternatives

In addition to the provisional Privacy Shield, alternatives are available for companies seeking to transfer data outside the EU. Since the invalidation of the Safe Harbor Framework, these alternatives have been much employed and discussed. Given that Privacy Shield may not be approved, especially if the Article 29 Working Party and Member State representatives do not find the safeguards and oversight on U.S. government collection of data sufficient, companies should consider the continued use of these options.

Standard Contractual Clauses ("SCC"), also known as Model Clauses, are clauses issued by the EC under the Data Protection Directive 95/46/EC. They are available from the EC's website and their inclusion in a contract establishes preapproval to transfer personal data from the EU and EEA to any jurisdiction, including the United States. SCC can be used for inter-company and intra-company transfers of data. Companies that do not regularly transfer a great deal of personal data outside the EU, and have already incorporated SCC into their contracts, may find that the additional steps and commitments required when self-certifying to Commerce are not worth the effort. However, SCC and Binding Corporate Rules ("BCR"), discussed below, may be vulnerable to the same criticisms that eventually invalidated Safe Harbor and are also under review by the Article 29 Working Party. They will continue to provide valid authority during the period of review.

BCR are an intra-company alternative to SCC. BCR must first be approved by the DPA in the Member States where the company will use the BCR for authority to transfer data. Afterwards, the multinational company at issue must adopt the BCR. The company can only use the BCR for transfers within itself. However, the cost for BCR is upfront, and BCR can introduce elements of flexibility for companies regularly transferring data internally. BCR may be supplanted by the Privacy Shield in some cases, but its attraction for multinational companies with locations beyond the EU and United States may remain.

Derogations, or exceptions, provide a limited number of reasons why, under the Data Protection Directive 95/46/EC, data transfers can take place from the EU to another country without adequate protections. These include consent or an important public interest. However, derogations' limited scope and the risk inherent in relying upon them mean they will not serve as a substitute for an enacted Privacy Shield.

The Privacy Shield makes little mention of these alternatives. The annex establishing the Ombudsperson Mechanism extends the coordination beyond just the Privacy Shield to SCC, BCR, Derogations, and Possible Future Derogations. The Privacy Shield agreement envisions SCC, BCR, and Derogations, and Possible Future Derogations as alternatives sources of authority to transfer personal data. This provides an opportunity for companies to choose which source of authority to rely upon, based on their own needs.

While not yet enacted, it is important to note that a new set of rules, the General Data Protection Regulation ("GDPR") is expected to replace the current Data Protection Directive 95/46/EC in 2018. Officials reached an agreement to enact these new rules late last year and they are expected to go into effect two years after the European Parliament and EU Member States formally adopt them in April this year. The GDPR strengthens privacy rules applied to entities outside the EU, imposes multi-million Euro fines for violations, codifies the "right to be forgotten," and requires parties who

have been breached to notify regulators within 72 hours, as well as some of the subjects of the breach. The GDPR would also create an overarching European Data Protection Board composed of the supervisory authorities from all Member States. The GDPR establishes a tiered approach to penalties for breach which enables the DPAs to impose very significant fines for serious infringements. Where the infringement involves the basic principles of processing, data subject rights, transfers of personal data, or non-compliance with an order by the supervisory authority an administrative fine of up to 20 million euros or up to 4% of annual worldwide turnover (whichever is the higher) may be imposed. Administrative fines for other specified serious infringements can be up to 10 million euros or up to 2% of annual worldwide turnover (whichever is the higher). The GDPR includes guidelines by which fines are to be assessed, by reference to the nature, gravity and duration of the infringement.

Recommendations

In light of the unsettled nature of the network of rules – both proposed and adopted – governing personal data transfers outside the EU, it can be challenging to determine the appropriate next steps for an organization. While not yet officially approved, the GDPR is expected to be formally adopted by the European Parliament and EU Member States this spring. King & Spalding recommends that companies transferring personal data from the EU to the United States should begin to prepare for GDPR compliance. Meanwhile, companies for which SCC and BCR have proved burdensome and a poor replacement for the Safe Harbor Framework, such as those dependent on cloud-based systems, may wish to act quickly should the Privacy Shield enter into force in order to benefit from the delayed implementation of rules governing data transfer to third parties.

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.