Privacy Shield Is Here. Now What?

On July 12, 2016, EU Commissioner Věra Jourová and US Secretary of Commerce Penny Pritzker held a signing ceremony for the EU-US Privacy Shield agreement, the much-anticipated framework for protecting and transferring personal data from the European Union to the United States. This ceremony followed the decision by the European Union's College of Commissioners that the Privacy Shield agreement provides an adequate level of privacy protection, as well as a vote by the collective of member states (known as the Article 31 committee) in support of the Privacy Shield. This means that the Privacy Shield has been recognized as providing an adequate level of protection to personal data transferred from the 28 EU member states (and the three European Economic Area member countries: Norway, Liechtenstein, and Iceland) to entities in the United States that certify to the Privacy Shield's privacy principles. Companies can certify their agreement to the Privacy Shield with the US Department of Commerce starting August 1 in order to support their transfers of data across the Atlantic, and there are advantages to certifying at the earliest possible date. Companies that certify in August and September will be given a nine-month grace period in which to bring their existing commercial relationships with third parties into conformity with the Privacy Shield principles.

The Long Road to Privacy Shield

After the Court of Justice of the European Union struck down a previous data transfer mechanism, the US-EU Safe Harbor framework in *Maximilian Schrems v. Data Protection Commissioner case (C-362-14)*, the European Commission and the US Department of Commerce stepped up their efforts to negotiate a new agreement that addressed the court's concerns that the Safe Harbor framework lacked sufficient safeguards to protect EU citizens' data from "massive and indiscriminate" bulk surveillance by the US government. On February 2, 2016, the negotiators announced that they had reached an agreement in principle and that the new framework for transatlantic exchanges of personal data would be called the EU-US Privacy Shield. One month later, the text of that agreement was released to the public, and Mayer Brown identified the enhanced commitments on data handling that US companies could elect to agree to by joining the Privacy Shield.

The draft text was then reviewed by the Article 29 Working Party (composed of EU Data Protection Authorities), the European Parliament and the European Data Protection Supervisor, who called for improvements to the text in order to better safeguard individual privacy as well as "future-proof" the Privacy Shield to ensure that it adapts to the EU's new General Data Protection Regulation ("GDPR"). The GDPR will take effect in May 2018, replacing the current Data Protection Directive 95/46, which sets out the rules for transfers of personal data from the EU to third countries.

Some privacy advocates in Europe—including Max Schrems, the Austrian law student who led

the charge against the Safe Harbor framework—have said that they would also challenge the Privacy Shield as insufficient to protect EU data privacy rights. In addition, the decision of the EU's high court in the case Mr. Schrems brought against the Safe Harbor framework found that member state data protection authorities have the independent authority to investigate complaints about the adequacy of methods of data transfer. This lays the groundwork for certain data protection authorities (such as perhaps those from the four countries abstaining from the Article 31 decision to approve the Privacy Shield: Austria, Croatia, Slovenia and Bulgaria) to conclude, on their own authority, that the Privacy Shield does not provide an adequate level of protection.

The Privacy Shield Principles

The European Commission adopted the "Implementing Decision" regarding the adequacy of the protection provided by the Privacy Shield and published annexes, including a package of materials from the US government describing the privacy principles along with commitments made by the relevant federal agencies. The new text of the privacy principles includes revisions to address the criticism of the data protection regulators in the European Union.

In order to use the Privacy Shield as a method for transferring data, a company must be subject to the jurisdiction of the US Federal Trade Commission or the US Department of Transportation, agencies with the authority to enforce the Privacy Shield framework. Companies under the jurisdiction of those agencies (a category that doesn't include, for example, banks and insurance companies) can certify, on an annual basis, to the US Department of Commerce and publicly commit to comply with the Privacy Shield principles. Following is a summary of the seven Privacy Shield privacy principles:

1. **Notice:** The Privacy Shield requires companies to publish a notice with information about the extent and purposes of their data collection and processing. Companies must also publicly declare that they participate in the Privacy Shield and must identify an independent dispute resolution body.
2. **Choice:** Companies must offer individuals a choice about whether their personal information can be disclosed to a third party or used for a purpose that is "materially different from the purpose(s) for which it was originally collected or subsequently authorized…." That choice can be opt-out for non-sensitive personal information, but for sensitive personal information the individual must provide their affirmative express consent (opt in). It is not necessary to provide a choice when the third party is acting as an agent "to perform task(s) on behalf of and under the instructions of the organization."
3. **Accountability for Onward Transfer:** The Privacy Shield strengthens protections of personal data that is transferred from a US company to a third party (regardless of whether the third party is located in the United States). All onward transfers of data must be (i) for limited and specified purposes, and (ii) pursuant to a contract; and (iii) the contract must provide the same level of protection as the Privacy Shield principles. This is the case even if the company transfers the data to a company certified to the Privacy Shield. An additional requirement stipulated in the Privacy Shield text is that the third party must notify the company if it can no longer meet its obligations under the contract, and this notification requirement must be a term in the parties' contract.
4. **Security:** Companies must take "reasonable and appropriate measures" to protect information.

5. **Data Integrity and Purpose Limitation:** The Privacy Shield includes a new requirement that US companies must limit personal information they obtain to the information that is relevant for the purposes of their processing[1] and may not process personal information in a way that is "incompatible with the purposes for which it has been collected or subsequently authorized by the individual." Companies can provide individuals with the right to opt-out of data processing where a new purpose is compatible with the original purposes. But a company cannot provide an opt-out mechanism only for processing that is incompatible with the original purpose. Companies must comply with the new data retention principle, which requires a company to delete personal data it no longer uses for its original or compatible purpose of processing. Companies may, however, retain information indefinitely if the dataset is held in a way that does not identify (or make identifiable) the individual.
6. **Access:** The Privacy Shield lays out additional rights that allow individuals to verify the accuracy of, or modify, the personal data held about them, except where the burden or expense of providing access would be disproportionate or if it were to violate another individual's privacy.
7. **Recourse, Enforcement, and Liability:** The Privacy Shield provides multiple layers for assuring compliance with the principles and providing recourse to individuals with consequences for companies. For example, companies are required to provide independent recourse mechanisms if they are not able to resolve an EU data subject's complaint, and they must select their independent resource mechanism prior to certifying to the Privacy Shield.

In addition to the Privacy Principles directed at companies, the new Privacy Shield also includes new assurances from the US government that their access to EU personal data for law enforcement and national security purposes is subject to clear limitations, safeguards and oversight mechanisms. The US government's commitments also include further information about the independence of the ombudsperson mechanism within the US State Department to handle and resolve complaints or inquires from EU individuals in the context of access to data by the US government for national security or law enforcement purposes.

The Impact of the GDPR and Brexit

The GDPR, which replaces Data Protection Directive 95/46, was adopted in May 2016 and will come into force throughout the EU in May 2018. Beginning on that date, data controllers located in countries outside the EU that process personal data in relation to offerings of goods or services to individuals within the EU, or as a result of monitoring individuals within the EU, will have to comply with the requirements of the GDPR. The Implementing Decision states that the Privacy Shield will not affect the application of the GDPR to the processing of personal data, which means that beginning in May 2018, companies that have certified to the Privacy Shield with respect to personal data transferred to them by other companies may also have to implement the requirements of the GDPR with respect to the personal data that they process about individuals in the EU more broadly. Additional obligations that a company that has already certified to Privacy Shield may have to comply with as a result of the implementation of the GDPR include the obligation to notify European data protection authorities and data subjects in the case of a security breach, the requirement to implement strong governance and oversight of the processing of personal data conducted within the company, including the requirement to appoint an independent data protection officer and conduct privacy impact assessments to assess, mitigate and record higher-risk processing of personal data in

certain circumstances and to implement "privacy by design" when initiating projects or tasks that will affect how personal data will be processed and protected by the company. This might be seen as unfortunate, but is the result of two different backgrounds. The GDPR came from the EU itself and is based on a desire to protect its citizens and adapt to changes in technology; it is data subject driven. In contrast, the Privacy Shield agreement was reached in the wake of the *Schrems* case and provides for periodic changes, paving the way for evolving requirements.

The United Kingdom's referendum to leave the EU (known as "Brexit") is raising additional concerns that the Privacy Shield may not apply to data transfers from the UK. At least in the short term, companies will be able to rely on the Privacy Shield as a mechanism for receiving personal data from the UK, as the United Kingdom is and will remain a member of the EU until negotiations on its exit are complete, which may take two years or longer. The UK's Data Protection Act 1998 (which implements the current Data Protection Directive 95/46) will remain in force until it is repealed and, assuming the United Kingdom is still a member of the European Union by May 2018, the GDPR will come into force in the United Kingdom. In the longer term, it is likely (but not certain) that Privacy Shield (or a scheme similar to Privacy Shield) will cover personal data received from the United Kingdom. Because of the significance of UK trade with the European Union and the United States, it is likely that the UK Parliament will either retain or adopt new legislation that is the same or very similar to European data protection legislation in order to ensure that the United Kingdom remains an adequate data protection regime as far as the European Commission is concerned. If the United Kingdom remains an adequate data protection regime, then that should allow companies that are certified to the Privacy Shield to receive personal data from the United Kingdom in accordance with its principles. However, if the UK does not remain an adequate data protection regime, then it is possible that the Privacy Shield may cease to apply to transfers of personal data received from the United Kingdom (including transfers of personal data sent from another European country via the United Kingdom).

The Bottom Line

Companies rely on data flows to provide online and mobile services to their customers and to transfer information about their employees, customers and suppliers. Having a valid mechanism in place by which to transfer data from the European Union to the United States is not only important to business but is a legal requirement enforced by governments on both sides of the Atlantic.

Since the Safe Harbor agreement was invalidated, companies have had to rely on alternative mechanisms for their data transfers, such as standard contractual clauses and binding corporate rules. These alternative methods fit well with certain business models, but other companies have urgently awaited this week's announcement of a final Privacy Shield agreement. Privacy Shield is the best option for many companies because it provides a relatively easy way to legally process the personal data of European customers and employees. In particular, companies that act as a controller or agent and receive data from many other Privacy Shield companies are effectively required to adopt the Privacy Shield principles in order to receive that data as a third-party. Those companies may find it more efficient to certify to the Privacy Shield. We also predict that, given the resources that went into finalizing the Privacy Shield, there will be certain Data Protection Authorities in the EU member states (though certainly not all) who will want to see companies adopt the Privacy Shield principles and will treat those principles as the gold-standard for data protection.

There is a risk that Privacy Shield will be struck down, but that risk is present for other forms of data transfer mechanisms as well. Currently pending before the Irish High Court is a challenge to the standard contractual clauses claiming that this method of data transfer also permits "massive and indiscriminate" surveillance of EU citizens' data by the US government. What this suggests is that companies waiting for long-term legal certainty in support of a certain type of data transfer may be waiting a long time. Nonetheless, companies should weigh the cost of coming into compliance with a particular method of transfer against the uncertainty that such a transfer won't always be available.

Companies can begin to certify to the Privacy Shield on August 1. They should start now with evaluating whether Privacy Shield is the right fit for them and, if so, should begin performing an internal assessment of what additional controls will be needed in order to comply with the enhanced privacy principles. Prior to certifying, companies are required to identify and register with an independent dispute resolution provider. There are advantages to certifying to the Privacy Shield early. Companies that certify in August and September will have up to nine months in which to bring their existing commercial relationships with third parties into conformity with the Privacy Shield principles. Companies that certify after the first two months will not be afforded the same grace period.

For more information about this topic, please contact any of the lawyers listed below.

Kendall C. Burman
Counsel
+1 202 263 3210
kburman@mayerbrown.com

Rajesh De
Partner
+1 202 263 3366
rde@mayerbrown.com

Rebecca S. Eisner
Partner
+1 312 701 8577
reisner@mayerbrown.com

Charles-Albert Helleputte
Partner
+32 2 551 5982
chelleputte@mayerbrown.com

Mark A. Prinsley
Partner
+44 20 3130 3900
mprinsley@mayerbrown.com

Lei Shen
Associate
+1 312 701 8852
lshen@mayerbrown.com

Oliver Yaros
Associate
+44 20 3130 3698
oyaros@mayerbrown.com

Endnote

[1] The principles give examples of compatible processing purposes as "those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, [and] preserving or defending the organization's legal rights…."