MAYER·BROWN

Tip of the Month: Why the Article 29 Working Party Rejected the EU-US Privacy Shield (and What to Do Now)

Scenario

A large company with offices in Europe and the United States had self-certified to adhere to the EU-US Safe Harbor framework and had been relying on it for the company's intra-company transfers of data—until the Court of Justice of the European Union (CJEU) struck down the framework last year. While the US government and the EU Commission proposed a new framework with stronger privacy protections—the EU-US Privacy Shield—to replace the invalidated Safe Harbor framework, the EU's Article 29 Working Party recently issued an opinion disapproving the Privacy Shield. The company's general counsel is not sure what the company will need to do to transfer data from the EU to the US now that the Safe Harbor framework has been invalidated and approval of the Privacy Shield has been put in doubt.

Background

In October 2015, the CJEU held that transfers of personal data from the European Union to the United States under the Safe Harbor framework were invalid, as those transfers did not ensure an adequate level of protection under European data protection law. In the aftermath of that decision, the EU Commission and the US government negotiated the Privacy Shield to improve the Safe Harbor framework and address the CJEU's concerns. A draft of the Privacy Shield was released in March 2016, and the Article 29 Working Party (a representative body of the EU data protection officers) then reviewed the Privacy Shield to see if it provided a level of protection equivalent to the EU Data Protection Directive and would protect the EU fundamental rights to private life and data protection. On April 13, 2016, the Working Party rejected portions of the Privacy Shield.

Overview of Opinion

While acknowledging that the Privacy Shield had made "significant improvements" to the Safe Harbor framework, the Working Party expressed strong concerns over whether the Privacy Shield would ensure a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed in the EU. In addition, some key data protection principles outlined in the EU Data Protection Directive were either not addressed or were inadequately substituted in the Privacy Shield.

Some of the Working Party's key concerns included:

- US surveillance law is not sufficiently clear or precise, and further clarification of important

limitations on intelligence collection is needed.

- The national security exceptions to the Privacy Shield may not be permissible, depending on proceedings currently before the CJEU on whether or not surveillance carried out by a European member state is unlawful.
- The Privacy Shield does not give the Ombudsperson sufficient independence or authority to provide EU citizens with redress on matters of US surveillance.
- The Privacy Shield is not clear regarding the need for data controllers to ensure that data is deleted once the purpose for which it was collected has become obsolete.
- The scope of the purpose limitation concept is not clear and applied inconsistently in some of the Privacy Shield's principles. It should be made clear that an organization cannot process personal data for a purpose that is materially different from and incompatible with the initial purposes for which the data was collected.
- There also is no protection in the Privacy Shield regarding automated decisions (i.e., the automated processing of personal data to evaluate certain aspects of an individual, such as his creditworthiness) that significantly affect an individual. The Working Party emphasized that this protection becomes even more crucial as new technologies are enabling more companies to consider the use of automated decision-making systems.
- Because the Privacy Shield will also be used to further transfer EU data from the US to a recipient in another country, such onward transfers must provide the same level of protection on all aspects of the Privacy Shield and not circumvent EU data protection principles.
- The Privacy Shield framework is currently "too complex." Because the principles and guarantees afforded by the Privacy Shield are set out in both the adequacy decision and in its annexes, information is both difficult to find and, at times, inconsistent.
- The Privacy Shield does not reflect several of the new principles contained in the new General Data Protection Regulation (GDPR), and, as a result, the Privacy Shield should be reviewed shortly after the GDPR becomes effective to ensure that the higher level of data protection offered by GDPR is reflected in the Privacy Shield.

What to Do Now?

Do not give up hope—an operational Privacy Shield framework is possible in the near future. The Working Party's opinion on the Privacy Shield is non-binding and advisory, and the EU Commission has shown signs that it is progressing with the next step for formally adopting the Privacy Shield, which is to obtain feedback from the Article 31 Committee (representatives of the member states). Companies should continue to use alternative transfer mechanisms (e.g., EU Standard Contractual Clauses and Binding Corporate Rules). However, companies should be aware that there may be future legal challenges to some of the alternate methods of transferring data on the same basis that the Safe Harbor framework was invalidated. Therefore, companies should follow any new developments closely.

Finally, there is not expected to be any grace period for companies if and when the Privacy Shield framework is finalized. Companies will be expected to comply immediately upon certification. However, companies that certify to the Privacy Shield framework in the first two months following its effective date will have nine months in which to bring their existing commercial relationships with third parties into conformity with the Privacy Shield principles.

For inquiries related to this Tip of the Month, please contact Kendall Burman at

kburman@mayerbrown.com or Lei Shen at lshen@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com, Ethan Hastert at ehastert@mayerbrown.com, or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.