Privacy Shield and Onward Transfer

When the European Court of Justice struck down the U.S.-EU Safe Harbor Framework last October, it set off a scramble by the U.S. and EU governments to find a suitable replacement to allow the free flow of personal data between the continents. What emerged was the Privacy Shield Framework – essentially the Safe Harbor on steroids. Like the Safe Harbor, the Privacy Shield allows U.S. companies to certify their own compliance with the applicable principles, but with enhanced data privacy requirements and oversight.

The Commerce Department opened the gates to Privacy Shield self-certification on August 1 of this year. Recognizing that one of the more challenging Privacy Shield principles is "accountability for onward transfer," the Commerce Department offered a sweetener for companies that self-certified by September 30: a nine-month grace period within which to comply with onward transfer requirements.

As under the Safe Harbor, the Privacy Shield onward transfer principle requires that if a U.S. company certified under the Privacy Shield is transferring data to a third party, such as a service provider, it may only do so if the third party follows adequate data protection principles. However, the requirements have been expanded beyond Safe Harbor.

Under the Privacy Shield, if there will be a transfer of personal information to a third party acting as a controller, the participant must "enter into a contract with the third party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual." If the third party is acting as an agent rather than a controller, the Privacy Shield participant itself must ensure that the transfer of data is only for limited and specific purposes. Whether the data transferee is a controller or an agent, the data must be provided the same level of protection as is required under the Privacy Shield principles.

There is an additional liability angle in the case of data transfers to agents. The Privacy Shield organization remains liable if its agent processes personal data in a manner inconsistent with the Privacy Shield principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

Privacy Shield-certified organizations should use the nine-month grace period to take a careful look at all of their third party contracts to ensure they are in compliance with the onward transfer principle, as well as evaluate the ability of their third party vendors to protect personal data consistent with the Privacy Shield. Because of the very specific onward transfer requirements of the Privacy Shield, in most cases a Privacy Shield organization's vendor and service provider agreements will need to be amended to satisfy the Privacy Shield principles.

Michael Whitener is a VLP Partner. His legal practice focuses on two areas: (1) technology transactions and (2) data privacy and cybersecurity. Michael provides practical advice on the collection, use, sharing and protection of data in compliance with an ever-changing network of privacy

laws. He conducts privacy audits and risk assessments, drafts privacy/security policies and data transfer agreements, advises on compliance with U.S. and foreign data privacy laws and regulations, and assists companies in preventing and responding to data security incidents.