Dead Before the Ink is Dry? EU Approves Privacy Shield Text

July 12, 2016

After months of uncertainty, the U.S. again has a framework of rules to follow that will govern U.S. business' use of EU residents' data. The European Commission approved the text of the EU-U.S. Privacy Shield (the "Privacy Shield") today. The Privacy Shield effectively replaces the EU-U.S. Safe Harbor mechanism, which was struck down in October of 2015. You can read about the European Court of Justice's opinion in this Client Alert.

If a company files its self-certification documents within two months from the day when the privacy shield became effective, it will be granted a nine-month grace period to bring its commercial contracts into conformity with the rules. During that transition period, the company must allow data subjects to opt out, and when personal data is transferred to a third party agent, it must ensure that the agent provides a level of protection consistent with the Principles.

As with Safe Harbor, companies can self-certify under the Privacy Shield to receive personal data from the EU and must annually re-certify to validate its participation.

The Privacy Shield requires that companies processing data of EU residents in the U.S. commit to comply with certain privacy principles to ensure an adequate level of protection for that data (collectively, the "Privacy Shield Principles"):

1. *Notice Principle*: organizations must provide information to data subjects relating to the processing of their data. A business must make its privacy policy public and provide links to (i) the Department of Commerce's website; (ii) the Privacy Shield List (all self-certifying organizations); and (iii) the Web site of an alternative dispute settlement provider of its choosing.

2. *Data Integrity and Purpose Limitation Principle*: personal data must be limited to what's relevant for the organization's purpose for processing it, reliable, accurate, complete and current. It may be retained in identifiable form for as long as it serves the purpose for which it was collected (with some limited exceptions for uses like journalism, art, and research).

3. *Choice Principle*: data subjects get the right to opt out if their data is to be used for a materially different (but still compatible) purpose than for which it was originally collected.

4. *Security Principle*: organizations must use reasonable and appropriate security measures to safeguard personal data.

5. *Access Principle*: data subjects shall have the right to know if an organization is processing their personal data and may correct, revise, or delete their personal data if inaccurate or processed in violation of the principles

6. *Recourse, Enforcement and Liability Principle*: organizations must provide robust mechanisms to ensure compliance with the Privacy Shield Principles and recourse for EU data subjects whose data has been processed in violation of them. To provide proper redress to EU residents, they agree to be subject to the investigative and enforcement powers of the Federal Trade Commission, the Department of Transportation, or another U.S. body. Organizations have to demonstrate they comply with the Privacy Shield Principles, either through self-assessment or outside audits.

7. *Accountability for Onward Transfer Principle*: the transfer of personal data of an EU resident from a complying organization to a third party outside the U.S. is only permitted for limited purposes and requires a contract between the parties requiring the transferee to abide by the Privacy Shield Principles.

One major concern the EU had with Safe Harbor was the lack of oversight and enforcement mechanisms. The Privacy Shield addresses the EU's concerns about a lack of oversight by:

- Creating a mechanism for dispute resolution;
- Having the Department of Commerce, the Federal Trade Commission, and the Department of Transportation commit to enforce the Privacy Shield for self-certified companies;
- Requiring the Department of Commerce to publicize a list of self-certifying organizations, which enforcement authority it must answer to, and a list of Privacy-Shield FTC enforcement cases;
- Removing organizations that persistently fail to comply with the Privacy Shield Principles and requiring they delete or return all EU personal data in their possession; and
- Providing that the Department of Commerce will conduct compliance reviews of self-certified organizations.

The Privacy Shield also includes enforcement and redress procedures:

- Gives EU data subjects the ability to lodge complaints against U.S. self-certifying organizations by requiring organizations to choose independent recourse mechanisms in the EU or the U.S. to field complaints and effectively enforce decisions;
- EU data subjects may file complaints with such independent recourse mechanisms, to EU data protection authorities, the Federal Trade Commission, or the Department of Commerce;
- If the foregoing have not resolved the data subject's complaint, he or she has the right to binding arbitration by the "Privacy Shield Panel," the rules for which are attached to the Privacy Shield text; and

- The Privacy Shield Panel provides non-monetary equitable relief, but the data subject may also pursue legal remedies under tort law and in cases of fraudulent misrepresentation, unfair or deceptive acts or practices, or breach of contract.

The EU's largest criticism with Safe Harbor, and the issue most threatening to the survival of the Privacy Shield, is the U.S. government's ability to access and use EU personal data under the auspices of national security and surveillance. The Privacy Shield states that the U.S. has affirmed the absence of indiscriminate mass surveillance, relying primarily on discrete searches. Bulk collection would only be used under specific conditions and must be as targeted and focused as possible. A newly created position of Privacy Shield Ombudsperson will handle complaints related to data used or accessed for national security purposes. He or she will be independent from the U.S. intelligence community.

Even before the first U.S. company is able to self-certify, critics are already condemning the Privacy Shield, claiming its provisions do not go far enough to protect EU personal data from the prying eyes of the U.S. government. Max Schrems, whose complaint is the subject of the case that killed Safe Harbor, has weighed in on the Privacy Shield and is certain it will be defeated in court.

Contact Information

To learn how your company can self-certify under the Privacy Shield, please contact Ted Claypoole at 704.331.4910 or TClaypoole@wcsr.com, Cameron Stoll at 843.860.2378 or CStoll@wcsr.com or any member of the Womble Carlyle Privacy and Data Protection Team.