Chicago Daily Law Bulletin®

Volume 162, No. 88 Serving Chicago's legal community for 161 years

Reworked EU-U.S. Privacy Shield still undergoing growing pains

When the European Union's highest court issued its October 2015 ruling striking down the U.S.-EU Safe Harbor framework, shock waves rippled on both sides of the Atlantic.

For thousands of U.S. companies handling the personal information of European citizens — as well as companies in the EU that send the personal data of European citizens to U.S. companies — the Schrems v. Facebook decision meant that they could no longer rely on self-certification under the U.S.-EU Safe Harbor framework to establish compliance with EU privacy laws.

EU data protection regulators gave negotiators from the EU Commission and the U.S. Commerce Department a drop-dead date of Jan. 31 of this year to negotiate a revamped framework after which they threatened enforcement actions against companies engaging in cross-border data transfer.

U.S. and EU negotiators blew the deadline, but took advantage of a couple of extra days to reach an agreement before a planned February meeting of EU data protection regulators. The EU Commission announced on Feb. 2 the U.S.-EU Privacy Shield or, as some have dubbed it, Safe Harbor 2.0.

While the announcement provided the general parameters of the privacy shield, the details of the actual framework remained cloaked in uncertainty until recently. On Feb. 29, the commission released details as to how the updated privacy shield will work.

U.S. companies are now subject to stronger obligations to protect the personal data of EU citizens and increased monitoring and enforcement by the U.S. Commerce Department and Federal Trade Commission in cooperation with European data protection authorities.

To rely on the privacy shield trans-Atlantic data transfer, U.S. companies must register annually to be on the privacy shield list and self-certify that they meet their obligations under the pact. Once a company self-certifies, its compliance with the principles is enforceable by the FTC.

Under the privacy shield, companies must display a privacy policy on their website and follow that privacy policy. In transferring, storing and processing the personal data of EU citizens, companies must adhere to the privacy principles enumerated in the agreement, including the following:

- Notice and transparency about the collection and use of personal information.
- Choice — providing an opt out for disclosure of data to third parties or for uses other than the original intended purpose.
- Compliance with rules relating to the onward transfer of data.
- Limitations on data processing to what is necessary and relevant to the purpose of the data collection.
- Allowing individuals access to and the ability to correct, amend or delete personal information where it is inaccurate or has been processed in violation of the privacy principles.
- Taking "reasonable and appropriate" measures to keep personal data secure.

One of the main issues the European court cited for its decision in Schrems was the lack of legal redress for EU citizens who believed their data had been mishandled by U.S. companies.

The privacy shield requires that companies reply within 45 days to any complaints and provide recourse for EU citizens, including an alternative dispute resolution solution, a free-of-charge program to which U.S. companies must join if they want to be privacy shield-certified.

If a complaint cannot be resolved by any other means, an arbitration mechanism ensuring an enforceable remedy will serve as a last resort. EU citizens may also go to their home data protection authorities, which will work with the U.S. Commerce Department or the FTC to investigate and resolve complaints.

The Commerce Department will be monitoring and actively verifying that the companies' privacy policies are presented in line with the privacy shield and are readily available.

Our country has also committed to maintaining an updated list of current privacy shield members and removing companies that have left the agreement. The Commerce Department will monitor any false claims of privacy shield participation or the improper use of the privacy shield certification mark (data protection authorities can refer organizations to the department for review) and will ensure that companies that are no longer members of the privacy shield program continue to apply "its principles to personal data received when they were in the privacy shield, for as long as they continue to retain them."

U.S. authorities have also pledged to ensure no indiscriminate or mass surveillance by national security authorities occurs. Our government has provided written commitments and assurance that access by public authorities to personal data transferred under the new arrangement for national security purposes will be subject to "clear conditions, limitations and oversight" to prevent generalized access, according to the commission.

This will be accomplished through the establishment by our country of a new ombudsperson to handle EU citizens' complaints or enquiries, which will operate independently of national security services.

The EU Commission and the Commerce Department will conduct the review to assess compliance with privacy shield principles. The review will utilize all sources of information available, including transparency reports by companies on the extent of government access requests.

The commission will also hold an annual privacy summit with nongovernment organizations and other stakeholders to discuss developments in U.S. privacy law and their impact on Europeans. At the conclusion of the review, the commission will issue a public report to the European Parliament and European Council.

To provide additional civil remedies for European citizens, Congress on Feb. 12 passed the Judicial Redress Act. The act, which President Barack Obama signed into law on Feb. 24, provides citizens of "covered" countries (and organizations such as the EU) the right to bring civil actions under the Privacy Act of 1974 for unlawful disclosure of their personal records by U.S. government agencies.

The Justice Department with the concurrence of the secretaries of State and Treasury (and the Homeland Security Department) will have the authority to designate the covered countries or regional organizations based on whether they have met several conditions:

- They have entered into an agreement with the United States providing appropriate privacy protections for sharing information with the United States (or otherwise demonstrated that they have effectively shared information with U.S. agencies while providing appropriate privacy protections).
- They permit the transfer of personal data for commercial purposes.
- The attorney general has certified that their policies do not materially impede the national security interests of the United States.

These designations may be revoked if the attorney general later determines that the covered country or organization no longer meets those conditions. Further, the attorney general's decisions are exempt from review.

It's now up to the Article 29 Working Party (representatives of the data protection authorities, the European data protection supervisor and the European Commission) to give its opinion on whether the EU-U.S. Privacy Shield can reliably protect data transferred to the United States.

Along with the rest of the information on the privacy shield, the commission released a draft adequacy decision indicating acceptance by the Article 29 Working Party.

The Article 29 Working Party was expected to meet this spring to take up the issue.

In the meantime, U.S. authorities are preparing for the implementation of the new framework. Companies that want to use the EU-U.S. Privacy Shield should be, too.

PRIVACY, TECHNOLOGY AND LAW

Nerissa Coyle McGinn

Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law as well as intellectual property law, focusing on trademark clearance and counseling.

Our government has provided written commitments and assurance that access by public authorities to personal data ..., will be subject to "clear conditions, limitations and oversight" to prevent generalized access ...