Cybersecurity Law Report
An Acuris company

cslawreport.com

April 13, 2022

DATA TRANSFERS

U.S., E.U. Announce Trans-Atlantic Data Privacy Framework: What Companies Can Do Now

By Elizabeth E. McGinn, Sasha Leonhardt and Lauren Bomberger, *Buckley LLP*

The White House and European Commission in late March 2022 announced a new agreement in principle for trans-Atlantic data flows – the Trans-Atlantic Data Privacy Framework – that would replace the E.U.-U.S. Privacy Shield.

The United States and European Union began negotiations on a new framework in 2020 after the Court of Justice of the European Union (CJEU) concluded that the U.S.-E.U. Privacy Shield was inadequate.

The new framework is the third attempt in the last 20 years to address data transfers between the U.S. and E.U. and is likely to face continued criticisms and legal challenges. While the exact language has not yet been released, the parties' statements to date point to some key conclusions that can help companies prepare for the final framework – and suggest areas to watch for further clarification.

See CSLR's series on navigating data transfers post-*Schrems II*: Challenges and TIAs (Feb. 23, 2022); and SCCs and Supplementary Measures (Mar. 2, 2022).

History of Privacy Shield

2000 to 2015: U.S.-E.U. Safe Harbor Framework

The need for a systematic method to transfer data from the E.U. to the U.S. in compliance with E.U. laws first arose following the European Commission's 1995 Directive on Data Protection, the precursor to today's GDPR. The 1995 directive was designed to protect the personal data of E.U. citizens by proscribing data transfers to non-E.U. countries whose privacy protections had not been deemed "adequate."

The U.S. government and European Commission in 2000 completed negotiations on the U.S.-E.U. Safe Harbor Framework, which the European Commission subsequently deemed 'adequate' that same year. Much like its successors, Safe Harbor relied on U.S. companies self-certifying compliance through the U.S. Department of Commerce (Commerce). However, Edward Snowden's 2013 disclosure of U.S. intelligence activities caused many to question whether Safe Harbor sufficiently protected E.U. citizens against U.S. government surveillance.

See "ECJ Hearing on Safe Harbor Challenges How U.S. Companies Handle European Data" (Apr. 8, 2015).

2015: *Schrems I*

Based upon the Snowden disclosures, Maximilian Schrems, an Austrian privacy activist, alleged that U.S. intelligence agencies could access his personal data. Schrems filed suit with the CJEU, which determined in 2015 that Safe Harbor was invalid because it did not adequately protect E.U. citizens from U.S. government surveillance and did not provide them sufficient legal redress.

2016 to 2020: U.S.-E.U. Privacy Shield

In 2016, the U.S. and E.U. began negotiating a replacement for Safe Harbor called "Privacy Shield." The goal was that the final Privacy Shield framework would comply with the stringent standards of the GDPR, which the E.U. had recently adopted, as well as with the 1995 directive. The European Commission announced in mid-2016 that Privacy Shield provided an adequate level of protection under E.U. privacy law.

Privacy Shield maintained the self-certification process of Safe Harbor but included additional rights and protections, such as an individual's right to opt out of disclosure of their personal data to third parties or for marketing purposes, and the right to access their personal data. Negotiators also sought to provide E.U. data subjects greater redress through a complaint-handling process and a new ombudsman position at the U.S. State Department. The U.S. intelligence agencies also signed written assurances that their access to E.U. data would be subject to certain limitations and requirements.

2020: *Schrems II*

Despite the U.S. intelligence community's assurances, Schrems revised his original complaint and challenged standard contractual clauses (SCCs) on the basis that they did not provide sufficient protection from U.S. government surveillance. Another privacy advocacy group also lodged a complaint with the CJEU against Privacy Shield.

In 2020, much like it did in 2013, the CJEU held that the European Commission's adequacy decision on Privacy Shield was invalid. Again focusing on the U.S. intelligence community, the CJEU determined that the U.S. government's data collection was neither necessary nor proportional to its surveillance needs. Additionally, the CJEU questioned the neutrality of the ombudsman and held that E.U. citizens could not obtain sufficient redress in U.S. courts, stating:

[E]ven where judicial redress possibilities in principle do exist for non-US persons, such as for surveillance under FISA, the available causes of action are limited … and claims brought by individuals (including US persons) will be declared inadmissible where they cannot show 'standing' …, which restricts access to ordinary courts …

The CJEU held that SCCs were still valid but said that data exporters must verify on a case-by-case basis the privacy requirements of the non-E.U. country to which they are exporting data. If the level of protection afforded is not equivalent to E.U. law, then an E.U. company may not export data.

The issues the CJEU cited in its Privacy Shield decision centered on actions by the U.S. government and left unchallenged most of the

obligations of U.S. companies under the framework. The government's Privacy Shield website also advises that the *Schrems II* decision "does not relieve participants in the E.U.-U.S. Privacy Shield of their obligations under the E.U.-U.S. Privacy Shield Framework." Given this, the Privacy Shield is still relevant for U.S. companies.

See "Ten Initial Steps for E.U. and U.S. Companies in Light of Schrems II Ruling" (Jul. 22, 2020).

Trans-Atlantic Data Privacy Framework: What We Know

The White House and European Commission described the Trans-Atlantic Data Privacy Framework (Framework) as the "culmination of more than a year of detailed negotiations between the E.U. and the U.S. following the 2020 decision by the [CJEU]." Aside from a fact sheet released by the White House and one-page white paper published by the European Commission, very little information has been released about the contours of the Framework.

The joint announcement demonstrates a clear commitment to resolving issues raised in Schrems I and II, including providing more robust protections and safeguards around U.S. government access to E.U. citizens' data and new mechanisms for redress.

The European Commission's one-page white paper highlights five principles:

1. Data should flow freely and safely between the E.U. and participating U.S. companies.
2. U.S. intelligence agencies should be subject to new rules and "binding safeguards to limit access to data" consistent with the necessary and proportionate principles espoused by the CJEU.
3. There should be a two-tier redress system for investigating E.U. citizens' complaints, including the creation of a new Data Protection Review Court.
4. The obligations imposed on U.S. companies should be "strong" and include the pre-existing self-certification requirements from Privacy Shield.
5. There should be specific monitoring and review mechanisms.

Although we may not see a draft of the Framework for some time, we anticipate that many of the changes from Privacy Shield will be targeted toward U.S. government actors. Because neither Schrems I nor II challenged the company-specific requirements or self-certification nature of prior data transfer frameworks, we would expect that much of the existing Privacy Shield compliance structure will remain in place. This may mean only limited adjustments are required for companies that were already complying with Privacy Shield.

What Can Companies Do Now?

Careful Monitoring

Because information about the Framework is so minimal, it is both likely and reasonable that most companies will wait for additional clarification. In the meantime, they will want to

consider consulting with qualified privacy professionals to monitor developments and consider how the new framework could yet again change the practices they have developed post-*Schrems II*.

Companies should prepare for another legal challenge by Schrems, who has already expressed skepticism regarding the agreement and said that he and his company would be scrutinizing it closely.

Review Past Enforcement to Identify Potential Compliance Challenges

Despite the possibility of further legal challenge, U.S. companies cannot entirely escape U.S. agencies' enforcement authority, and there has been no suggestion that the new Framework will completely replace Privacy Shield. Many of the previous requirements for U.S. companies will likely remain in place.

The Federal Trade Commission in a March enforcement action against CafePress and Residual Pumpkin Entity LLC alleged, among other issues, that the company had allowed its certification to lapse despite representations in its privacy policy that it was compliant with Privacy Shield. Of note, the agency stated:

Although the European Court of Justice determined on July 16, 2020 that the EU-US Privacy Shield framework was not adequate for allowing the lawful transfer of personal data from the European Union and the Swiss Data Protection and Information Commissioner determined on September 8, 2020 that the Swiss-US Privacy Shield framework was similarly inadequate, those decisions do not change the fact that Residual Pumpkin represented to consumers that it was certified under both Privacy Shield frameworks, and as such, would fully comply with the Principles . . . .

Companies in the past have ended up in hot water for failing to certify or re-certify properly. In another notable case, the FTC brought an enforcement action against NTT Global Data Centers, Inc., an operator of secure data centers, alleging it made misleading statements to consumers by representing it had been certified by the Commerce Department when, in fact, its certification had lapsed. The FTC also alleged that NTT had failed meet other requirements under Privacy Shield, including (1) conducting annual verifications regarding its statements about its Privacy Shield practices, (2) maintaining a dispute resolution process, and (3) protecting, deleting or returning data under the program. In order for companies to ensure compliance with Privacy Shield, the FTC recommended that companies:

1. keep statements regarding Privacy Shield certification status up to date by ensuring self-certification is current;

2. fully comply with all provisions of the framework and not just on a piecemeal basis;

3. complete re-certification annually as certification lapse has been a primary enforcement focus; and

4. take orderly steps to withdraw from Privacy Shield, which requires certain procedures and ongoing duties to ensure compliance for any remaining covered data.

Given the legal risks under U.S. law and uncertainty under E.U. law, it is important that companies engage compliance and legal professionals who have experience with Privacy Shield, the GDPR and the E.U.'s data transfer requirements. Furthermore, companies that intend to pursue the new framework should ensure that their compliance management systems and policies and procedures demonstrate a real commitment to compliance as part of their everyday business operations.

Finally, in addition to the above steps, we continue to closely monitor the White House and European Commission for further developments as U.S. and E.U. negotiators finalize the Framework.

See "European Data Protection Supervisor Offers Advice on Privacy Shield Review and GDPR Preparation" (May 3, 2017).

Elizabeth E. McGinn, CIPP/US, is a partner in the Washington, D.C., and New York offices of Buckley LLP. She focuses her practice on assisting clients in identifying, evaluating and managing the risks associated with cybersecurity, internal privacy and information security practices, as well as those of third-party vendors. A significant part of her practice involves addressing data security breaches, working proactively with clients to prevent data security breaches and responding to regulatory inquiries, investigations and enforcement actions related to privacy, information security and cybersecurity issues.

Sasha Leonhardt, CIPP/US, CIPM, is a partner in Buckley's Washington, D.C., office. He represents financial services industry clients in a broad range of enforcement, litigation and regulatory matters with a focus on privacy and data security issues. Mr. Leonhardt assists clients with compliance matters as well as resolving government investigations and enforcement actions before a wide variety of federal and state agencies.

Lauren Bomberger is an associate in the Washington, D.C., office of Buckley LLP where she assists financial services clients on a variety of regulatory, enforcement, and transactional matters.