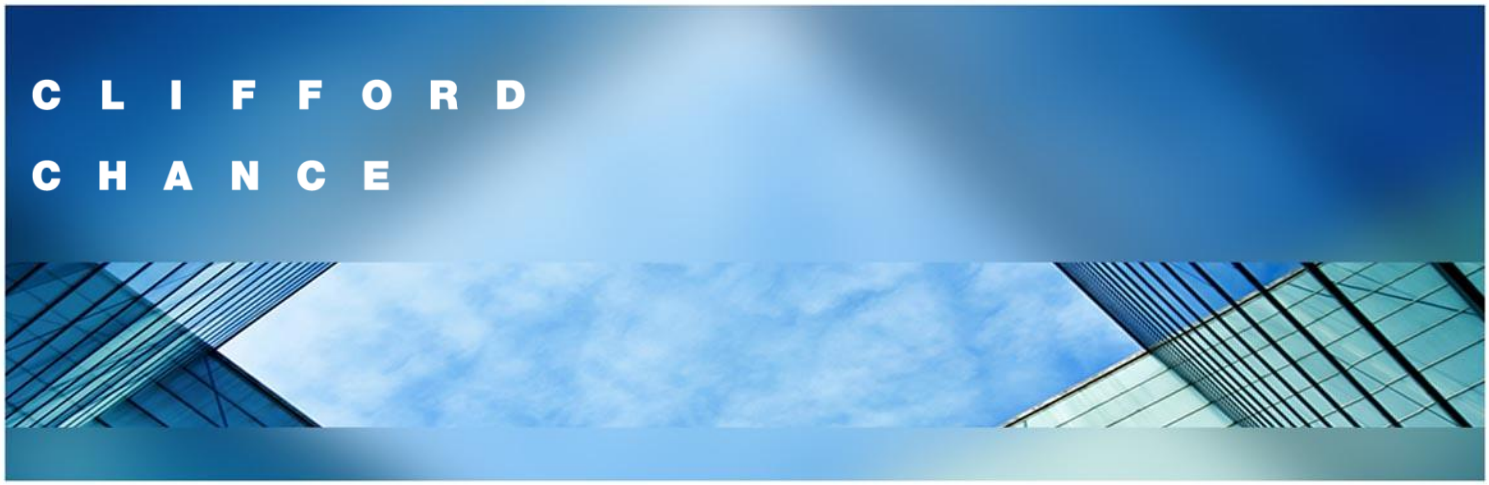

US AND EU AGREE ON FRAMEWORK FOR PRIVACY SHIELD REPLACEMENT

On March 25, 2022, US President Biden and European Commission President Ursula von der Leyen announced that the United States and European Commission have agreed in principle to a Trans-Atlantic Data Privacy Framework. This new framework aims to address deficiencies identified by the Court of Justice of the European Union ("CJEU") in *Schrems II*, which struck down the EU-US Privacy Shield over concerns regarding US surveillance programs and a lack of grievance mechanisms available to EU citizens. While the agreement is still "in principle" and specific details have yet to be determined, if approved, this agreement will reimplement an important legal mechanism necessary to facilitate data transfers between the European Union and the United States.

BACKGROUND

Trans-Atlantic data flows between the United States and European Union account for over $1 trillion in cross-border commerce each year, but recent legal developments have jeopardized this cross-border data flow. While the US and EU's trade interests have long been aligned, their approaches to data privacy differ. In the EU, privacy of communications and personal data protection are fundamental rights, a view reflected most recently in the expansive General Data Protection Regulation ("GDPR"). The US, on the other hand, does not have a comprehensive federal data privacy law; rather, it has a patchwork of state and federal laws that apply to certain sectors and in a handful of states.

These differing approaches to data privacy have come into sharp contrast in the context of cross-border data transfers. Under the GDPR, data may be transferred outside of the European Economic Area (EEA)[1] if the country to which it is headed has an "adequate" level of protection. An "adequate" country is one that has laws in place that the European Commission has determined provide equivalent

[1] The European Economic Area is an area of free trade and free movement of peoples, consisting of all 27 European Union countries, as well as Iceland, Liechtenstein, and Norway.

protections to those afforded by the GDPR. In the absence of an adequacy determination by the European Commission, data can only be transferred to a non-EEA country if: (i) "appropriate safeguards" are put in place (e.g., standard contractual clauses and appropriate supplementary measures described further below) or (ii) based on a derogation (e.g., explicit consent of the individual).

SAFE HARBOR AND PRIVACY SHIELD

To facilitate data transfer under these regulations, the US and EU have previously operated under two different international agreements.

From 1998 to 2015, the EU and US operated under the Safe Harbor Privacy Principles ("Safe Harbor"), which allowed for cross-border transfers so long as the US companies engaging in such transfers self-certified that they were in compliance with seven basic privacy principles and other requirements necessary to meet EU protection standards. But in 2015, the CJEU invalidated the Safe Harbor in *Schrems v. Data Protection Commissioner ("Schrems I"),* finding that the Safe Harbor framework did not adequately protect the privacy rights of EU citizens, primarily due to US national surveillance practices and a lack of redress mechanisms available for aggrieved data subjects.

To replace the Safe Harbor, the EU and US agreed to the Privacy Shield framework in 2016. Like the Safe Harbor, under the Privacy Shield, companies were required to self-certify compliance to several privacy principles. In addition, to address the CJEU's concerns raised in Schrems I, the Privacy Shield agreement included assurances from the US government that it would put limitations on access to personal data of EU citizens. It also implemented two redress mechanisms: (i) an ombudsperson responsible for handling complaints by EU citizens against the US government; and (ii) a binding arbitration process for complaints against private companies.

This framework was in place until 2020, when it too was struck down by the CJEU in *Irish Data Protection Commissioner v. Facebook and Maximillian Schrems ("Schrems II").* The CJEU held that the European Commission's determination that the US could ensure an adequate level of protection under the Privacy Shield framework was incorrect. Specifically, the CJEU raised concerns that the US government's foreign intelligence surveillance activities under Section 702 of the Foreign Intelligence Surveillance Act[2] and E.O. 12333[3] lacked limitations to ensure the surveillance programs abided by the GDPR's principle of proportionality, which requires data collection be no more than what is "strictly necessary." Additionally, the CJEU found that the ombudsman was an ineffective redress mechanism for individuals whose personal data was subject to US surveillance activities.

DATA TRANSFERS POST-*SCHREMS II*

The CJEU's *Schrems II* decision immediately invalidated the Privacy Shield, stripping the ability of companies to transfer data under this framework. To compensate, many companies have implemented EU-approved standard contractual clauses ("SCCs"), under which companies that receive personal data

[2] Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702") allows the US government to issue compulsory directives to electronic communications service providers to provide communications related to foreign targets.

[3] E.O. 12333 gives US intelligence agencies broad authority to engage in "signals intelligence" surveillance, which involves the collection of data from various sources, including foreign communications, radar, and other electronic systems, without court approval.

from the EEA commit to apply EU-equivalent data protection standards to personal data they receive, even when not required by their home country's laws. The *Schrems II* decision upheld SCCs as a valid transfer mechanism under the GDPR but required companies to conduct transfer impact assessments to determine whether additional safeguards need to be put in place to ensure adequate levels of privacy protection. Complying with these SCC requirements can be burdensome and costly, often requiring companies to hire external experts to assist with data mapping and legal assessments. The European Data Protection Board has also cautioned that for some data transfers (such as routine intra-group data transfers in the clear to non-EEA countries that do not meet EU law data protection standards), SCCs may simply not be sufficient to ensure adequate data protection.

Additionally, recent challenges to existing SCCs used by Google and Facebook have raised concern about the legal status of these agreements. In January and February 2022, Austria and France, respectively, declared Google Analytics's data transfers to the US illegal, finding the supplementary measures implemented after *Schrems II* were still not enough to exclude the possibility that US surveillance agencies could access EU citizens' data.[4]

TRANS-ATLANTIC DATA PRIVACY FRAMEWORK

Since *Schrems II*, the US and the EU have been negotiating to create a replacement for the Privacy Shield. While the prospect of a replacement seemed bleak for much of 2021, rumors began circulating of a potential breakthrough earlier this year. Then on March 25, 2022, US President Joe Biden and European Commission President Ursula von der Leyen announced an agreement "in principle" for a new Trans-Atlantic Data Privacy Framework.

Although specific details on how the framework will operate are still being worked out, the announcement indicates that the framework will reflect a balance between the US and EU's concerns for national security, privacy, and data protection. To address issues raised by *Schrems II*, under the new framework, the US has committed to:

- ensure signals intelligence collection may only be undertaken where it is necessary to advance legitimate national security objectives, and must not disproportionately impact the protection of individual privacy and civil liberties;
- establish a new multi-layer redress mechanism that will include an independent Data Protection Review Court made up of individuals chosen from outside the US government who will have full authority to adjudicate claims and order remedial measures; and
- require US intelligence agencies to adopt procedures to oversee new privacy and civil liberty standards.

The new framework will also incorporate core aspects of the previous Privacy Shield program. Participating companies will again have to adhere to and certify compliance with the Privacy Shield Principles. The new framework will also provide EU citizens with access to several different recourse mechanisms to

[4] For more on the French regulator's decision, please see our Talking Tech blog post here.

resolve complaints against participating companies, including binding arbitration and alternative dispute resolution.

TAKEAWAYS

The Trans-Atlantic Data Privacy Framework represents a continued commitment to ensuring there is a reliable mechanism in place to facilitate cross-border data transfers between the US and EU, but there is still much more work to be done. The United States and European Commission continue to work on translating the framework into a specific agreement that both sides will need to adopt—a process that could still be months from completion. Once the US has formally implemented these measures (likely through an Executive Order), there will then be a multi-step EU adequacy process—an initial adequacy determination by the European Commission, a non-binding opinion by the European Data Protection Board, and finally, approval by at least 55% of the EU Member States representing at least 65% of the total EU population.

Adequacy process aside, the Framework will also likely face scrutiny by privacy advocates. Maximillian Schrems, a privacy lawyer and the lead litigant in *Schrems I and Schrems II*, has stated that he will closely review the Framework as further details are revealed—and that he will not balk at bringing a challenge to the CJEU again if he finds the agreement is inadequate to protect the privacy rights of EU citizens. The European Data Protection Board has also issued a statement stating it will "analyse in detail" the reforms relating to proportionality and necessity and will examine the new redress mechanism closely to ensure it respects the rights of EU citizens to an effective remedy for violations of their privacy rights.

Other legal developments may also raise hurdles for the approval process. In March 2022, the US Supreme Court decided in *FBI v. Fazaga* that the government may continue to employ the state secrets privilege in cases brought by individuals alleging illegal government surveillance under FISA. Privacy advocates have argued that the decision may make it harder for EU citizens to bring challenges against FISA surveillance in US courts. It remains to be seen what impact this decision will have on the CJEU's further review of the redress mechanisms established by the Framework.

The Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), passed by the US Congress in 2018, may be another complicating factor in approving the Framework. Like the US intelligence community's ability to collect foreign data under FISA 702 and E.O. 12333, the CLOUD Act authorizes US law enforcement agencies to issue subpoenas or search warrants to obtain data stored outside the US from US-based service providers. It also establishes a framework for foreign governments to enter into agreements with the US to facilitate cross-border data transfers for law enforcement purposes.[5] Although the CJEU did not address the CLOUD Act in *Schrems II*, it may consider this legislation in a potential future challenge to the Framework. Privacy advocates have argued that data collection under the CLOUD Act raises privacy concerns and should require additional safeguards and better redress mechanisms. Though service providers may raise challenges to CLOUD Act warrants in US courts, the European Data Protection

[5] On March 22, 2022, the US and Canada announced that they had entered into formal negotiations for a bilateral agreement under the CLOUD Act. Having already signed CLOUD Act Agreements with the UK and Australia, Canada is now the third country to pursue such an agreement with the United States.

Supervisor and European Data Protection Board have raised doubts as to whether such challenges are sufficient to protect the rights of European citizens. Further, if the Framework is enacted, companies may find it difficult to transfer data from the EU in response to a CLOUD Act warrant while also abiding by the robust safeguards required by the Framework.

So, while the prospect of a new Framework is great news for companies that routinely transfer data from the EEA to the US, for now companies must continue to rely on SCCs (and upgrade to the European Commission's new SCCs by December 27, 2022 at the latest) and other transfer mechanisms to ensure they comply with the GDPR. The White House has suggested that the Framework will likely be aligned with the Privacy Shield Principles. Companies can review their existing data privacy practices against those required under the Privacy Shield Principles to ensure they are ready for certification under the new framework when it is approved.

CONTACTS

AMERICAS

Megan Gordon
Partner
Washington DC

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Daniel Silver
Partner
New York

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Michelle Williams
Partner
Washington DC

T +1 202 912 5011
E michelle.williams
@cliffordchance.com

Brian Yin
Associate
New York

T +1 212 878 4980
E brian.yin
@cliffordchance.com

Shannon O'Brien
Law Clerk
New York

T +1 212 880 5709
E shannon.obrien
@cliffordchance.com

EUROPE

Fernando Irurzun
Partner
Madrid

T +34 91 590 4120
E fernando.irurzun
@cliffordchance.com

Dr. Ines Keitel
Partner
Frankfurt

T +49 69 7199 1250
E ines.keitel
@cliffordchance.com

Jonathan Kewley
Partner
London

T +44 207006 3629
E jonathan.kewley
@cliffordchance.com

Simon Persoff
Partner
London

T +44 207006 3060
E simon.persoff
@cliffordchance.com

Dr. Gunnar Sachs
Partner
Dusseldorf

T +49 211 4355 5460
E gunnar.sachs
@cliffordchance.com

Dessislava Savova
Partner
Paris

T +33 1 4405 5483
E dessislava.savova
@cliffordchance.com

Jaap Tempelman
Senior Counsel
Amsterdam

T +31 20 711 9192
E jaap.tempelman
@cliffordchance.com

Grégory Sroussi
Counsel
Paris

T +33 1 4405 5248
E gregory.sroussi
@cliffordchance.com

Andrea Ferrari
Counsel
Milan

T +39 02 8063 4435
E andrea.tuninettiferrari
@cliffordchance.com

Andrei Mikes
Senior Associate
Amsterdam

T +31 20 711 9507
E andrei.mikes
@cliffordchance.com