GUNDERSON DETTMER

Data Privacy Insight: EU Approves New Framework for Transatlantic Data Flows; Uncertainty Remains

Insights
July 11, 2023

The European Commission has approved the new EU-U.S. Data Privacy Framework for transatlantic transfers, three years after the invalidation of its predecessor, the EU-U.S. Privacy Shield. Companies can soon sign up with the U.S. Department of Commerce to self-certify adherence to the Framework and benefit from this new cross-border transfer mechanism.

On July 10, the European Commission formally approved the new EU-U.S. Data Privacy Framework (the "Framework"), ushering in what many hope will be an era of free-flowing transatlantic data transfers. European entities will now be able to transfer personal data to Framework participants in the U.S. without having to put in place additional data protection safeguards or use the Standard Contractual Clauses for data transfers. In the coming days, the U.S. Department of Commerce will launch a new website for the Framework, where companies can self-certify as participating organizations.

Why is the Framework needed?

The General Data Protection Regulation ("GDPR"), which regulates the processing of Europeans' personal data, restricts the transfer of such data from the EU to countries that do not offer an adequate level of protection without a compliance mechanism in place. Washington and Brussels have collaborated twice before to achieve such an adequacy designation for the U.S.—first on the U.S.-EU Safe Harbor Framework, and then the EU-U.S. Privacy Shield—but their efforts in both cases were undone by

successful court challenges concerning electronic spying by American intelligence agencies.

In an attempt to address some of these concerns, the Biden administration issued Executive Order 14086 late last year on "Enhancing Safeguards for United States Signals Intelligence Activities." That order is designed to limit access to data by U.S. intelligence agencies; enhance oversight of activities of U.S. intelligence activities; and establish an independent redress mechanism, including a new Data Protection Review Court, to investigate and resolve complaints regarding access to such data. These safeguards will enhance the protection of transatlantic data flows overall, applying not only to transfers within the Framework but also to transfers relying on other tools, such as the Standard Contractual Clauses.

What do companies have to do to benefit from the Framework?

Under the Framework, participating companies must self-certify compliance with detailed privacy obligations, including with respect to purpose limitation, data minimization, data retention, and specific obligations for data security and sharing with third parties. The Department of Commerce, which will monitor whether participating companies meet the necessary requirements, is expected to provide further information on how to self-certify under the new Framework, including guidance to those companies that continued to adhere to the EU-U.S. Privacy Shield even after its invalidation. As with the Privacy Shield, compliance by certified companies will be enforced by the U.S. Federal Trade Commission.

Will this Framework be subject to legal challenges like its predecessors?

The now-approved Framework has been criticized for lacking clarity, and is certain to face legal challenges. Nyob, an organization headed by Max Schrems who championed both successful challenges to the prior transatlantic frameworks, indicated it would challenge the Framework, adding that the "third attempt of the European Commission to get a stable agreement on EU-U.S. data transfers will likely be back at the Court of Justice (of the European Union) in a matter of months." However, any legal challenges in the European courts will likely take some time (possibly several years), and many are optimistic that the Framework has a better chance than its predecessors to withstand such challenges.

Where can I find more information about the Framework?

Review the Adequacy Decision, the Factsheet and the Questions and Answers, each as provided by the European Commission. We will update this alert with further

information on the self-certification process from the U.S. Department of Commerce when available.

If you have any questions regarding this client alert or need assistance with evaluating the best path forward for your business, please reach out to your Gunderson Dettmer attorney or contact one of our data privacy experts:

Anna Westfelt (650) 463-5367 awestfelt@gunder.com

Cecilia Jeong (646) 490-9094 cjeong@gunder.com

Frida Alim (415) 801-4921 falim@gunder.com

James Gately (617) 648-9313 jgately@gunder.com

Related People

Anna C. Westfelt
PARTNER
P +1 650 463 5367

Cecilia Jeong
ASSOCIATE
P +1 646 490 9094

Frida Alim
ASSOCIATE
P +1 415 801 4921

James W. Gately
ASSOCIATE
P +1 617 648 9313

Related Services

Data Privacy

Featured Insights

PUBLIC VENTURES

Trump Executive Order Targets Proxy Advisors Over DEI and ESG Influence

EVENTS

Webinar: Paradigm Shift? Mandatory Securities Arbitration and the Impact of the SEC’s Recent Policy Statement for Companies and Investors

FIRM NEWS

Amidst Strong Year, Gunderson Dettmer Elects Nine New Partners

EVENTS

Webinar: AI in the Workplace: Legal Challenges and Best Practices

FIRM NEWS

2025 CVCA Annual General Meeting & Private/Venture Capital Summit in Beijing

CLIENT NEWS

Gunderson Dettmer Represented Hims & Hers in Acquisition of Livewell

CLIENT NEWS

Replicate Bioscience Announces Collaborative Agreement with Instituto Butantan

CLIENT NEWS

Gunderson Client Neptune to Be Acquired by OpenAI

CLIENT NEWS

Hims & Hers Announces Definitive Agreement to Acquire YourBio Health

CLIENT NEWS

LotusFlare Announces Equity Investment from Ericsson

PUBLIC VENTURES

SEC Chair Charts Disclosure Overhaul to Revive IPOs: Materiality and Scale Over ‘Regulatory Creep’

CLIENT NEWS