Updates
September 07, 2022
US-UK Bilateral Data Sharing Agreement Comes Into Force on October 3

Under a new agreement between the United States and the United Kingdom, communications service providers in the United States may soon begin to receive legal process directly from law enforcement agencies in the United Kingdom. U.S.-based recipients of this legal process may find it unfamiliar and may be uncertain as to how to respond.

The United States and the United Kingdom executed the agreement, known as a Data Access Agreement (the Agreement), under the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). The CLOUD Act allows the United States to enter into such bilateral agreements that allow law enforcement officials in each country to seek data from communications service providers in the other. The United States' agreement with the United Kingdom is the first of such and enters into force on October 3, 2022.

Under the agreement, U.S. communications service providers may start receiving legal process directly from U.K. law enforcement agencies demanding subscriber data and communications. U.K. providers can likewise anticipate receiving similar demands directly from U.S. law enforcement agencies. This is because, in 2019, the United States and the United Kingdom signed the Agreement (formally known as the Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime)—a first-of-its-kind agreement designed to overcome blocking statutes, remove conflicts of law, and facilitate cross-border criminal investigations involving communications data. After nearly three years, the United States and the United Kingdom announced in July 2022 that the Agreement would enter "into force" on October 3, 2022. Additionally, a similar agreement between the United States and Australia has been signed and is undergoing domestic approval processes. Negotiations between the United States and Canada are also underway.

The Agreement is a boon for the U.S. and the U.K. law enforcement. In essence, the Agreement will speed the process by which law enforcement of one country can obtain the data located in the other from many months to potentially a matter of days. It will also have significant practical effects on "covered providers" in both regions,

as well as companies that use such providers to house private information. Many covered providers are familiar with responding to domestic requests, but domestic laws (particularly in the United States) previously insulated covered providers from many of the burdens and risks associated with legal process issued by a foreign nation and seeking communications data. Now, covered providers will (for the first time) need to prepare for an influx of cross-border demands for communications data that have the force of law. Many U.S.-based providers will have questions about the volume and cadence of demands emanating from the United Kingdom, the format of the demands, and the proper procedure for addressing improper or unduly burdensome demands. U.K. providers will undoubtedly have the same questions about United States' legal process. On both sides of the Atlantic, covered providers that receive data from European data subjects will have questions about how the Agreement may affect their obligations under European data protection law. And all providers and other stakeholders (such as privacy and civil liberties advocates) may wonder about potential gaps, how the Agreement matches up to other cross-border disclosure regimes, and whether there are opportunities to improve upon this and future agreements.

Because this is the first bilateral agreement under the CLOUD Act set to enter into force, many of these questions remain unexplored territory. But there is a lot we know in the interim, and this series of posts will demystify the CLOUD Act, the Agreement, and their likely effects by exploring the following questions:

- What is the Agreement, and why does it matter?
- How might the Agreement impact companies' obligations under European data protection law?
- How does the Agreement compare to other existing cross-border paradigms?

This Update is the first in a series.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Data Security Counseling and Breach Response Communications

Related insights

Update

Two Tools for Trump To Dismantle Biden-Era Rules: the Regulatory Freeze and the Congressional Review Act

Update

The FY 2025 National Defense Authorization Act: What’s New for Defense Contractors