wiley

ALERT

New DOJ Restrictions on Cross-Border Data Transactions Take Effect April 8: Ten Questions as Your Business Prepares to Comply

March 5, 2025

The U.S. Department of Justice's (DOJ) sweeping new rule on cross-border data transactions is set to take effect in substantial part next month, with broad implications for companies that transfer U.S. personal data or government-related data abroad. The DOJ issued the new rule – "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons" (the Rule) – on January 8, 2025, and it imposes strict prohibitions on certain data transfers outside the U.S., as well as detailed privacy, cybersecurity, and data governance restrictions on a broader set of transactions outside the U.S.

At a high level, the Rule prohibits or restricts U.S. individuals or entities from engaging in transactions involving bulk U.S. sensitive personal data or government-related data with countries of concern (including China) or covered persons (including entities that are related to countries of concern, for example, foreign entities that are 50% or more owned by a country of concern). The new Rule adopts novel and potentially broad definitions of key threshold terms, so it will have wide-ranging impacts on U.S. companies that conduct commercial transactions internationally.

The bulk of the Rule will take effect on April 8, 2025, with certain due diligence, audit, and reporting requirements taking effect on October 6, 2025. Given this impending deadline, below, we answer 10 key questions about the Rule's new requirements, to help companies assess the new Rule and develop a compliance strategy.

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Lori E. Scheetz
Partner
202.719.7419
lscheetz@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Practice Areas

Export Controls and Economic Sanctions
FTC and Consumer Protection
National Security
Privacy, Cyber & Data Governance

1. What are the countries of concern? The Rule identifies China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela as countries of concern. While this is the current list, the Rule allows for this list to be amended on a prospective basis by the DOJ, with concurrence from the Secretaries of State and Commerce.

2. Who are covered persons to which restrictions apply? The Rule establishes an expansive definition of "covered person," which borrows from the Department of the Treasury, Office of Foreign Assets Control's (OFAC) "50 Percent Rule." Specifically, the definition of a "covered person" includes, but is not limited to, the following entities and individuals:

- Entities organized or chartered under the laws of a country of concern or having their principal place of business in a country of concern.
- Entities 50% or more directly or indirectly owned, individually or in the aggregate, by one or more countries of concern or covered persons, such as a government of a country of concern; a company organized in a country of concern; or an individual primarily resident in a country of concern. This would capture, for example, a French company that is 50% or more directly or indirectly owned by a company incorporated in China or an individual primarily resident in Venezuela.
- A foreign individual who is primarily resident in a country of concern or who is an employee or contractor of a country of concern or covered entity (regardless of their foreign citizenship or foreign country of birth).
- An individual or entity, including persons located in the United States and other U.S. persons, designated as a covered person by the Attorney General, as well as their 50% owned entities.

3. What data is covered by this Rule? This Rule applies generally to two types of data: (1) bulk U.S. sensitive personal data, and (2) government-related data.

Sensitive personal data includes six broadly defined categories: covered personal identifiers, precise geolocation data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination of those categories. DOJ has defined these categories differently from other privacy frameworks, and companies should closely assess to determine if data they handle is considered "sensitive" under this new framework. The Rule generally applies only to data transactions involving sensitive personal data that exceed certain bulk volume thresholds.

Government-related data is defined as either: (1) any precise geolocation data for any location within any area enumerated on DOJ's Government-Related Location Data List, or (2) any sensitive personal data that a transacting party markets as linked or linkable to certain personnel associated with the United States government, including the military and Intelligence Community. The Rule covers that government-related data regardless of volume.

4. What transactions are impacted by this Rule? The Rule establishes a new regulatory framework for "covered data transactions," which are those that involve any access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data and that involve "data brokerage," vendor agreements, employment agreements, and investment agreements. The Rule defines data brokerage broadly to include "the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or a vendor agreement, involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data." This is more expansive than a similar federal data brokerage law – the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA) – that Congress enacted last year. Accordingly, companies should assess whether their international data transactions could be considered to be data brokerage transactions under the new Rule, even if companies are not considered to be "data brokers" under other frameworks.

5. What transactions are prohibited? The Rule establishes several prohibitions, including those that affect transactions that do not directly involve a country of concern or covered person. With respect to "data brokerage" transactions, it prohibits such transactions involving bulk sensitive U.S. data or government-related data either (1) to a country of concern or covered person, or (2) to *any foreign person* – even those that are not countries of concern or covered persons – if the transaction does not include contractual and reporting safeguards that are aimed to prevent potential onward transfer of covered data from the foreign person to a country of concern or covered person. Because of the breadth of these prohibitions, companies that engage in international data transfers out of the U.S. should review and develop compliance for those transactions, not just those specifically involving countries of concern.

The new Rule also prohibits transactions that would give access by a country of concern or covered person to bulk human 'omic data or human biospecimens, and it generally prohibits actions to evade, avoid, cause a violation of, or attempt or conspire to violate the Rule.

6. What transactions are restricted, and what restrictions does the Rule impose? The Rule also establishes a category of transactions that are restricted. These include covered data transactions involving vendor agreements, employment agreements, or investment agreements with a country of concern or covered person.

If a transaction is restricted, the company must implement an extensive set of requirements, including new Cybersecurity and Infrastructure Security Agency (CISA) security requirements, which establish organizational-level, system-level, and data-level requirements. Other requirements for restricted transactions include due diligence, audit, recordkeeping, and reporting requirements.

7. What transactions are exempt? The Rule establishes several categories of transactions that are exempt from some or all of the requirements of this Rule. Companies should assess these exemptions carefully to understand their scope and impact. Exempted transaction categories, some of which overlap with OFAC's sanctions-related exemptions, include:

- Personal communications;
- Information or informational materials;
- Travel;
- Data transactions, other than those involving data brokerage, to the extent they are ordinarily incident to and part of the provision of telecommunications services;
- Investment agreements subject to the Committee on Foreign Investments in the United States (CFIUS) mitigations;
- Financial services;
- Corporate group transactions;
- Drug, medical device, and biological product authorizations;
- Clinical trials regulated by the U.S. Food and Drug Administration;
- Transactions required by federal law such as those on international civil aviation; and
- Official U.S. government activities.

8. Are there reporting obligations? There are broad reporting requirements under the new Rule. For example:

- The Rule includes a broad requirement applicable to "every person" to furnish reports on demand to DOJ.
- The Rule requires an annual report for certain restricted transactions involving cloud-computing services.
- The Rule requires reporting by any U.S. person that has received and affirmatively rejected an offer from another person to engage in a prohibited transaction involving data brokerage, again borrowing from an OFAC concept (i.e., OFAC's requirement to report transactions rejected for sanctions-related reasons).

9. How will the Rule be enforced? The Rule will be enforced by the DOJ, which may investigate potential violations, including holding hearings, deposing witnesses, and issuing subpoenas for witnesses and documents. Violators could face civil and criminal penalties, including fines and imprisonment.

10. Will the DOJ provide any additional parameters or guidance? Similar to OFAC's licensing approach for sanctions matters, the Rule provides an opportunity to utilize a general license issued by DOJ (i.e., a broad authorization that does not require a company to obtain any additional, special permission from the U.S. government to engage in a transaction within the scope of the authorization) or apply for a specific license for a transaction otherwise prohibited or restricted. DOJ can publish a general license where, for example, multiple companies in the same industry submit requests for specific licenses on the same topic, or in circumstances where DOJ otherwise learns of a need to issue a general license, such as via industry engagement. Specific licenses, on the other hand, are limited to the applicant company and the specific facts in the application. Licenses likely will be limited to transactions that the U.S. government views as lower risk

and/or consistent with U.S. interests. Indeed, in its commentary to the final rule, DOJ noted that it "anticipates that licenses will be issued only in rare circumstances as the Department deems appropriate." There is also an opportunity to seek advisory opinions on concrete data transactions that may be subject to prohibitions or restrictions. Finally, the DOJ stated when it issued the Rule that it "anticipates issuing public guidance on compliance with, and enforcement of, the rule before its effective date."

***

Wiley's Privacy, Cyber & Data Governance, International Trade, and National Security practices assist companies in navigating complex privacy, security, digital trade, data localization, trade controls, and related issues. If you have any questions, please contact one of the attorneys listed on this alert.