PUBLICATION

DOJ Final Rule Targets Cross-Border Data Transfers: Key Implications for U.S. and Foreign-Owned Companies Operating in the U.S.

Authors: Vivien F. Peaden, Alisa L. Chestler
April 08, 2025

In the final days of the Biden administration the U.S. Department of Justice (DOJ) issued a sweeping set of regulations which are in effect as of today, April 8, 2025. The regulations focus on cross-border data transfers for personal data. The final DOJ Rule, titled "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons" (DOJ Rule), introduces significant restrictions and prohibitions on data transactions involving specific foreign countries. The DOJ Rule casts a wide net, impacting a broad range of activities from M&A and real estate deals to employment agreements, data licensing, and supplier management. With data exposure now elevated from a privacy issue to a national security concern, companies across sectors must reassess their cross-border engagements and compliance strategies.

What's Changed:

This Rule aims to prevent certain countries of concern, including China, Russia, Iran, North Korea, Cuba, and Venezuela—from accessing sensitive personal data and government-related information. The journey to this final rule began with a series of executive orders (EO) from the Biden administration. While some speculated it might be paused or reversed by the Trump administration, no action was taken and presumably the DOJ will enforce restrictions against data flows to certain foreign actors that are classified as "**prohibited transaction(s)**" or "**restricted transaction(s)**".

What's in the DOJ Rule?

The final DOJ Rule has broad implications for U.S. businesses handling and potentially inadvertently transferring personal data or government-related information. Specifically, the DOJ seeks to regulate the following:

Country of Concern: The DOJ Rule initially designates six nations as "countries of concern": China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela.

Covered Person: The DOJ Rule restricts and/or prohibits the following "**Covered Person**" from accessing certain government-related information and U.S. sensitive personal data:

1. Foreign entities that are 50 percent or more owned by, organized under the law of, a Country of concern, organized under the laws of, have their principal place of business in a Country of Concern;

2. Foreign entities that are 50 percent or more owned (directly or indirectly) by Covered Persons (either individuals or entities).

3. Foreign Individuals, who are non-US residents working as employees or contractors of a Country of Concern or a Covered Person;

4. Foreign individuals primarily residing in Countries of Concern.

5. Other entities or individuals as reasonably determined by the Attorney General based on certain criteria.

Covered Data: The DOJ Rule primarily focuses on six (6) categories of personal data and two (2) categories of government-related information:

- Sensitive Personal Data above a certain volume threshold (**Bulk U.S. Sensitive Personal Data**), which is broadly defined to include the following:

Human genomic data

Biometric identifiers (e.g., facial images, voice prints and patterns, and retina scans)

Personal health data (e.g., the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. The term includes basic physical measurements and health attributes (such as bodily functions, height and weight, vital signs, symptoms, and allergies); social, psychological, behavioral, and medical diagnostic, intervention, and treatment history; test results; logs of exercise habits; immunization data; data on reproductive and sexual health; and data on the use or purchase of prescribed medications.)

Personal financial data (e.g., information related to an individual's credit, debit cards, bank accounts, and financial liabilities, including payment history)

Precise geolocation data

Certain **covered personal identifiers** that in combination with other data can be linked or linkable to other sensitive personal data (e.g., names linked to Media Access Control (MAC) addresses from devices, first and last name linked to an email and IP address, among others), subject to certain exemptions.

- Government-related Information *regardless of* data processing volume:

Precise geolocation data of certain sensitive government locations or geographical areas identified in the DOJ Rule's schedule;

Sensitive personal data that is linked to or linkable to current or former employees or contractors of the U.S. government.

Covered Data Transactions: The DOJ Rule establishes sweeping prohibitions and restrictions on data transactions that could grant access to U.S. sensitive personal data or government-related information by

certain foreign actors, with implications spanning M&A, real estate, employment, higher education, and commercial vendor agreements.

1. **Restricted Transactions**: Subject to certain exemptions, the DOJ Rule restricts any U.S. entities or individuals from knowingly engaging in the following three (3) categories of transactions with a Covered Person or a Country of Concern unless the U.S. person entering into the transactions complies with certain "security requirements:"

- Employment Agreement, including board-level, executive-level arrangements or services, and other employment arrangements, excluding those for independent contractors.
- For example, companies with foreign operations in Countries of Concern, such as China or Russia, may need to expressly restrict foreign employees from accessing Covered Data. These restrictions further limit U.S. companies from outsourcing certain functions to Countries of Concern if these activities involve accessing Covered Data or AI-related data training.
- Investment Agreement, including any transactions, acquisitions of direct or indirect ownership interests in U.S. real estate, U.S. legal entities, excluding passive investment, certain stock investment, or investment where a Covered Person is a minority shareholder or limited voting rights.
- For example, a Chinese technology company enters into a shareholder's agreement with a U.S. business that develops data centers or mobile apps that process Covered Data. Such investment may be a restricted transaction if it provides the Chinese investor the right to access such Covered Data.
- Vendor Agreement, including cloud-computing services, software-as-a-service subscriptions, HR Payroll or Recruiting platforms, AI-enabled chatbots, AI contract management services, data sharing arrangements, AdTech services, mobile app development, management consulting services, business process outsourcing arrangements, and other IT or non-IT related services involving data access and transfers, among others.
- For example, companies with foreign operations in Countries of Concern, such as China or Russia, may need to expressly restrict foreign employees from accessing Covered Data. These restrictions further limit U.S. companies from outsourcing certain functions to Countries of Concern if these activities involve accessing Covered Data or AI-related data training.

2. **Prohibited Transactions**. The DOJ Rule prohibits knowingly engaging in data transactions that provide a Country of Concern or Covered Person access to certain Covered Data, involving:

- Data Brokerage refers to sales of data, data licensing, or similar commercial transactions involving data transfer from data provider to data recipient.
- This prohibition potentially requires all organizations to examine their licensing agreements to identify and assess potential concerns. Companies should conduct due diligence on data recipients, licensees, or customers when providing data access to certain foreign actors or entities with ties to Countries of Concern.
- For data transactions involving data brokerage with foreign parties that are not a Covered Person, such data transfers require additional contractual obligations and reporting obligations.
- Data transactions involving access to bulk **human biometric data or human biospecimens** from which such data can be derived.

These prohibitions and restrictions are poised to have a wide impact on a broad range of commercial activities and legal practices. From **corporate transactions** involving cross-border investors and data center transactions, to **real estate acquisitions** with foreign ownership interests, **employment agreements** involving foreign nationals residing in Countries of Concern, and **supplier management** in sectors like technology

licensing, healthcare, and financial services—nearly every corner of a business' operations may be subject to the DOJ enforcement.

What Penalties will U.S. Businesses face for violations?

Violations can result in civil penalties up to the greater of $368,136 or 2X the amount of transaction involved. Willful violations can lead to criminal fines of up to one million USD ($1,000,000) and up to 20 years imprisonment.

What Immediate Steps should U.S. Businesses take?

Organizations should promptly undertake comprehensive reviews of their data handling practices and international engagements. Key steps include:

3. Assess Data Transactions: Identify whether your organization collects or processes Covered Data as defined by the DOJ Rule.

4. Evaluate Foreign Interactions: Determine if any Covered Persons or foreign actors have access to your data or systems; and in some instances, report **within 14 days** of becoming aware of certain known or suspected outbound data transfer involving government-related information and sensitive personal data.

5. Review Third-Party Relationships: Closely monitor your IT or other supplier engagements, M&A transactions, real estate transactions, employment arrangements, and investment partnerships to ensure compliance with the DOJ Rule.

6. Obtain License with DOJ, if qualified**.** U.S. businesses may apply with the DOJ for general licenses to authorize certain data transactions. Upon approval, such U.S. business will conduct such approved Covered Data Transactions subject to specific terms and conditions approved by the DOJ and undertake additional reporting obligations mandated by the DOJ.

7. Build Compliance Program for Restricted Transactions: By **October 6, 2025**, any U.S. Persons engaging in Restricted Transactions must

- Develop and implement a data compliance program, including risk-based procedures for verifying regulated data flows, a program to verify vendor identity and compliance, and written policies describing security requirements that meet certain standards.

- Conduct an annual audit by an independent auditor regarding its compliance under the DOJ Rule covering the preceding 12 months. Such audit report must be retained for at least 10 years.

For more information or assistance on this topic, please contact Alisa Chestler, CIPP/US, QTE, Vivien Peaden, AIGP, CIPP/US, CIPP/E, CIPM, PLS, or a member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.