



LEGAL UPDATES

New DOJ Limits on Cross-Border Data Transfers Prompt Assessment by Businesses

04/02/2025 | 4 minute read

On April 8, the National Security Division of the U.S. Department of Justice's (DOJ) new rule on cross-border data transfers takes effect. It restricts U.S. businesses from transferring certain bulk sensitive personal data to entities owned, controlled or subject to the jurisdictions of China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and/or Venezuela – defined as "countries of concern."

Why This Matters

If your business processes **biometric, financial, healthcare, location, or genetic data**, you may be affected by this new rule ("[Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons](#)"). Violators of the transfer rule can face civil penalties up to the greater of \$368,136 or twice the amount of the transaction. Willful violations can result in a fine of up to \$1,000,000, up to 20 years in prison, or both. Now is the time to evaluate your risk exposure, update contracts and implement safeguards to protect your business.

The DOJ's new rule, alongside evolving global data regulations such as the EU GDPR, China's PIPL, and U.S. privacy laws such as HIPAA, FERPA, and various state laws including the CCPA, introduces significant operational, legal and compliance challenges for businesses handling sensitive personal data.

Who Needs to Know

The new DOJ rule applies broadly to U.S. persons and entities engaged in the export of bulk sensitive personal or bulk government-related data to "countries of concern" or "covered persons," but the key sectors likely impacted include:

- **Data Brokerage Firms** — Entities involved in the sale or licensing of access to data. The rule prohibits U.S. persons from engaging in data brokerage transactions with covered persons involving bulk sensitive personal data or any amount of U.S. government-related data.

Related People

Megan M. Miller, CIPP/E

Associate
Chicago
312.920.3315
megan.miller@lathropgpm.com

Tedrick A. Housh, III, CIPP/US, CIPP/E

Partner
Kansas City
816.460.5642
tedrick.housh@lathropgpm.com

Chiara Portner, CIPP/US

Partner
Redwood Shores
650.804.7672
chiara.portner@lathropgpm.com

Related Services

[Data Privacy & Cybersecurity Compliance](#)

Related Sectors

[Financial Institutions](#)
[Health Care](#)
[Life Sciences](#)
[Technology](#)

- **Technology and Telecommunications Companies** — Firms that manage, process, or transfer significant volumes of sensitive personal data, such as precise geolocation information, personal health records or biometric identifiers.
- **Healthcare and Biotech Organizations** — Institutions handling human genomic data or biospecimens. The rule prohibits transactions involving bulk human omic data with countries of concern or covered persons.
- **Financial Institutions** — Organizations processing personal financial data, including bank account details and credit card information.
- **Government Contractors** — Companies with access to U.S. government-related data, including geolocation data of sensitive locations or information linked to former government employees.

If your company is in one of these sectors, you will next want to consider whether the sensitive data is in “bulk” or if it discloses the locations of government activities or concerns employees of the US government.

What is “bulk” sensitive information? It depends on the type of data and the number of persons or devices at issue. For example, human genomic data of more than 100 persons is “bulk,” as is precise geolocation for more than 1,000 devices and personal financial information of more than 10,000 persons. (The complete list is found in Section 202.205 of the rule.)

There is no bulk threshold for data showing the locations of government activities or for data on U.S. government personnel. (Think of smartwatch data showing the location of U.S. intelligence personnel, for example).

The DOJ’s new rule expressly references prohibited vendor or employment agreements, giving five examples in each category. In Section 202.217(b), the rule prohibits an agreement that employs global IT operations team members in countries of concern who would have access to the U.S. company’s systems containing bulk human genomic data. In Section 202.258, a prohibited vendor agreement would send bulk precise geolocation information to a vendor headquartered in a country of concern to process for storage and processing. Although there may be exceptions for such agreements, such as an intra-company transfer by a global corporation, companies should tread carefully.

What You Can Do

Here are some practical steps you can employ to address three types of risk associated with the new DOJ data transfer limits:

1. Overlapping Global Data Transfer Risks

Even if businesses comply with the DOJ rule, they must also navigate broader international data privacy laws like GDPR and China’s PIPL.

✓ *Practical Actions*

- Companies storing EU employee or customer data in the U.S. must ensure a compliant transfer mechanism, such as the US-EU/UK/CH Data Privacy Framework certification or Standard Contractual Clauses (SCCs).
- Firms handling Chinese consumer data need government approvals under PIPL before transferring data abroad.
- Businesses subject to CCPA must disclose and address foreign data use restrictions and sharing practices.

2. Heightened Risks for AI, AdTech and Data-Driven Businesses

AI companies training models on large datasets, adtech firms tracking user behavior, and data brokers selling consumer information may face severe restrictions on their operations. Notably, the rule applies even if the data is anonymized, pseudonymized, de-identified or encrypted.

✓ *Practical Actions*

- AI firms should evaluate data sources and remove any datasets originating from restricted countries.
- Adtech companies must review tracking and profiling technologies to avoid non-compliant data-sharing.
- Data brokers may need to divest certain data assets or adjust collection practices to avoid regulatory scrutiny.

3. Stricter Vendor and Third-Party Management

Businesses should audit vendors and partners to ensure they're not transferring restricted data to China, Russia, Iran, North Korea, Cuba or Venezuela – whether directly or indirectly via subsidiaries.

✓ *Practical Actions*

- Require vendors to certify compliance with DOJ restrictions in contracts.
- Implement enhanced due diligence for foreign-owned cloud, IT and data analytics providers.
- Establish continuous monitoring of data flows to detect non-compliant transfers.

Key Takeaway: Proactive Compliance is Critical

The new DOJ rule is just one piece of a much larger puzzle. Companies must now take a holistic approach to data governance – ensuring compliance with multiple jurisdictions, evolving AI regulations and industry-specific requirements. Start today to develop a compliance strategy that ensures your operations remain secure and legally sound.

If you have questions about the impact of this new DOJ data transfer rule, please contact [Tedrick Housh](#), [Chiara Portner](#), [Megan Miller](#), or your regular Lathrop GPM attorney.