Hashed & Salted | A Privacy and Data Security Update
September 2025

The DOJ's New Bulk Data Transfer Rule: What Every Business Needs to Know—and Do—Now

In a sweeping move to bolster national security and safeguard sensitive information, the U.S. Department of Justice (DOJ) has introduced a transformative regulation: the Bulk Data Transfer Rule. While the rule took effect in April, certain affirmative compliance obligations—such as due diligence, audits and reporting—become enforceable starting Oct. 6, 2025. This rule marks a significant shift in how American businesses must manage the flow of personal and government-related data—especially when that data could end up in the hands of countries of concern.

Whether you're a hospital administrator, a fintech executive or a general counsel at a manufacturing firm, this rule likely applies to you.

Why This Rule Matters

The DOJ's new regulation is not just another compliance box to check. It's a direct response to growing concerns about the exploitation of U.S. data by certain foreign governments. The rule aims to prevent large-scale transfers of sensitive data to countries deemed national security risks—including China, Russia, Iran, North Korea, Cuba and Venezuela.

Who Is Affected?

Contrary to what some may assume, this rule is not limited to tech giants or data brokers. It applies to all U.S. persons and entities—regardless of industry—if they transfer or allow certain countries and entities to access bulk U.S. sensitive personal data or U.S. government-related data.

What Data Is Covered?

The rule focuses on two key categories:

1. **Sensitive Personal Data:** This includes names, addresses, biometric identifiers (like fingerprints or facial scans), precise geolocation data, health records and financial information about U.S. residents. This definition is substantially broader than definitions of "sensitive personal information" under existing U.S. state comprehensive privacy laws.
2. **U.S. Government-Related Data:** This includes information about U.S. government employees, contractors and certain geolocation data tied to government facilities.

The rule applies only when this data is transferred in bulk. The thresholds vary, as detailed below.

Attorney Advertising

Bulk Data Thresholds by Data Type

Data Category	Threshold for Bulk Data
Biometric Identifiers	≥ 1,000 U.S. Persons
Human Genomic Data	≥ 100 U.S. Persons
Other Human "-omic" Data (e.g., epigenomic, proteomic, transcriptomic)	≥ 1,000 U.S. Persons
Precise Geolocation Data	≥ 1,000 U.S. Devices
Personal Financial Data	≥ 100,000 U.S. Persons
Personal Health Data	≥ 100,000 U.S. Persons
Covered Personal Identifiers (e.g., name, address, phone number)	≥ 100,000 U.S. Persons
Government-Related Data (defined as any precise geolocation data relating to a list of over 700 geofenced areas near government facilities, and sensitive personal data that is marketed as linkable to employees, contractors or officials of the U.S. government)	Any volume, if it pertains to current or former U.S. government employees, contractors or military/intelligence personnel

These thresholds are cumulative and apply regardless of whether the data is collected directly or indirectly and whether it is transferred in a single transaction or over time as part of a broader arrangement. Where a transfer includes more than one category of data in combination, the lowest applicable threshold applies.

Where Can't the Data Go?

The rule affects data transactions involving six countries: China, Cuba, Iran, North Korea, Russia and Venezuela. It also applies to individuals and entities with specific connections to these jurisdictions—in some cases, even if they operate elsewhere. The rule applies a nuanced definition for these "covered persons" that requires close scrutiny of residency, employment status and a company's corporate structure.

Entities that fall within the definition of "covered person" are automatically in-scope for the rule. In addition, the DOJ will publish and maintain a Covered Persons List identifying individuals or entities that the agency has designated as covered persons. Businesses are expected to screen vendors and partners against this list.

What's Prohibited—and What's Just Restricted?

The rules do not apply to every potential transaction, but certain "covered data transactions" are categorized as either prohibited or restricted.

1. **Prohibited Transactions:** Most bulk transfers of covered data to the listed countries or their affiliates are banned outright.
2. **Restricted Transactions:** Restricted transactions include certain vendor, employment and investment agreements with a country of concern or a covered person. In limited cases, these kinds of transfers may be allowed—but only if stringent security and

compliance measures are in place, as outlined by the Cybersecurity and Infrastructure Security Agency. These measures include specific contractual provisions prohibiting onward transfer to covered persons or countries of concern, and periodic certifications of compliance.

What Are the Penalties?

The penalties for noncompliance are:

1. Civil penalties of up to $377,700 per violation or twice the value of the transaction—whichever is greater.
2. Criminal penalties for willful violations, including fines of up to $1 million and up to 20 years in prison.

What Should Businesses Do Now?

The DOJ granted a 90-day "good faith" implementation period, ending July 8, 2025. That deadline has now passed, meaning businesses are expected to be in full compliance with the rule. The DOJ stated that during the initial period, it would not prioritize civil enforcement if businesses were making demonstrable good faith efforts to comply. Now, however, enforcement actions may proceed for noncompliance. This underscores the urgency for organizations to ensure their data practices align with the rule's requirements.

Here are steps businesses can take toward becoming compliant:

1. **Map Your Data**

- Identify what sensitive or government-related data you collect and store.
- Understand how it flows—internally, to vendors and across borders.

2. **Review Your Partners**

- Assess whether any third parties you work with are based in—or have ties to—the restricted countries.
- Screen all vendors using the DOJ's forthcoming Covered Persons List.

3. **Update Contracts and Policies**

- Amend contracts to prohibit unauthorized data transfers.
- Include DOJ-compliant language and require partners to notify you of any relevant data sharing or changes in ownership.

4. **Build a Compliance Program**

- Designate a responsible officer or team.
- Develop policies for monitoring, recordkeeping and annual certification.

5. **Document Everything**

- Maintain detailed records of your compliance efforts, audits and due diligence—for at least 10 years.
- Refer to the DOJ's Compliance Guide and Frequently Asked Questions for sample language and best practices.

Conclusion

The DOJ's Bulk Data Transfer Rule is a landmark development in U.S. data protection and national security policy. Its broad scope and strict penalties mean that businesses must be proactive about data governance. By taking proactive steps now—mapping data, vetting partners, updating contracts and building a robust compliance program—businesses can mitigate the risk associated with bulk data transfers subject to the rule.

Related Professional

Eyvonne Mallett . . . . . emallett@loeb.com