JANUARY 27, 2025

DOJ Final Rule on Bulk Data Transfers Implements New Restrictions on Transferring Personal Data Out of the United States

by Meghan K. Farmer , Henry W. Tharpe

The U.S. Department of Justice (DOJ) has issued a final rule that significantly restricts the transfer of bulk sensitive personal data and government-related data to certain foreign entities deemed countries of concern. Effective as of April 8, 2025 (with certain diligence and audit provisions taking effect in October), this rule came as a part of the Biden Administration's broader strategy to protect U.S. national security and mitigate risks posed by cross-border data flows, particularly to certain countries, such as China. The rule defines concepts like "sensitive data" and "covered transaction" broadly, so many companies that do business in covered jurisdictions will face new compliance obligations.
However, the recent transition to the Trump Administration in has introduced a degree of uncertainty regarding the future of the rule. Under the Administration's January 20, 2025, memorandum imposing a regulatory freeze pending review, all new and pending regulations, including the DOJ's rule, will be subject to additional scrutiny. This review raises the possibility of amendments, delays, or even rescission of the new DOJ rule, creating a dynamic compliance environment for businesses. Given the complexity of compliance, companies must prepare to meet the rule's requirements while monitoring for potential changes in its implementation.

Overview of the DOJ Final Rule

The final rule, promulgated under the authority of Executive Order 14034 (Protecting Americans' Sensitive Data from Foreign Adversaries), establishes a comprehensive framework for scrutinizing and, where necessary, restricting or prohibiting the transfer of sensitive data to certain foreign persons. This regulatory development reflects the government's growing concern over how foreign adversaries could exploit U.S. data to undermine economic competitiveness, individual privacy, and national security. Below we highlight the rule's major provisions and compliance obligations.

Key Provisions of the DOJ Rule

1. Broad Scope of Data Coverage

The rule defines "bulk sensitive personal data" expansively to include data sets that can be used to identify U.S. persons or reveal sensitive personal information. The definition takes into account both the types and amounts of data involved in a transaction. Transactions involving sensitive data are regulated only when the transaction exceeds "bulk" thresholds specified in the rule. Categories of covered data include:

- Health and Genetic Data: Medical records, genetic information, and biometric identifiers such as fingerprints and facial recognition data.

- Financial Information: Banking details, credit card numbers, and other personally identifiable financial data.
- Government-Related Data: Information pertaining to U.S. government employees, military personnel, and contractors, as well as data related to government operations. This includes any precise geolocation data for any location listed on the DOJ's expanded Government-Related Location Data List, which enumerates 738 government-related locations. Additionally, the definition includes sensitive personal data that is linkable to current or former U.S. government employees, contractors, or senior officials.

The rule applies to different categories of U.S. sensitive data sources at various numeric thresholds:

- Precise Geolocation Data: More than 1,000 U.S. devices
- Biometric Identifiers: More than 1,000 U.S. persons
- Personal Health Data: More than 10,000 U.S. persons
- Personal Financial Data: More than 10,000 U.S. persons
- Covered Personal Identifiers: More than 10,000 U.S. persons
- Human 'Omic Data: More than 1,000 U.S. persons (but for human genomic data, more than 100 U.S. persons)

2. Restrictions on Transfers to Covered Jurisdictions

The rule designates certain foreign nations, including China, as jurisdictions that pose heightened risks to national security. Transfers of covered data to entities in these jurisdictions are subject to stringent scrutiny and, depending on the nature of the information, outright bans. This provision reflects concerns over foreign governments' use of data to support espionage, economic coercion, or other hostile activities. Other countries of concern include Cuba, Iran, North Korea, Russia, and Venezuela.

3. Prohibited Transactions

The DOJ's final rule categorically prohibits U.S. persons from engaging in two primary types of data transactions unless exemptions apply, or a license is granted. The rule bans any data brokerage transactions involving access to covered data by countries of concern, described above, or covered persons. Covered persons include certain foreign entities or persons designated as national security threats. Any data brokerage transaction involving access to covered data by such entities is strictly prohibited. Second, the rule categorically prohibits transactions that involve access by a country of concern or covered person to "bulk human genomic data" and "bulk human 'omic data." These terms include transactions involving access to human genomic data from over 100 U.S. persons, and human epigenomic, proteomic, or transcriptomic data from over 1,000 U.S. persons, or the corresponding biospecimens from which such data could be derived, respectively.

4. Restricted Transactions

The rule imposes additional restrictions on certain transactions involving sensitive data, even if those transactions are not prohibited outright. These restricted transactions apply to scenarios where foreign recipients may gain access to government-related data or bulk sensitive personal data, discussed above. Any transaction that allows a foreign person to access U.S. government-related data is prohibited

unless the foreign recipient is contractually obligated to prevent subsequent prohibited transactions. Transactions involving bulk sensitive personal data are restricted unless the U.S. party imposes contractual safeguards on the foreign recipient and complies with certain audit, recordkeeping, due diligence, and security obligations outlined below:

- **Audit Obligations:** The rule requires annual audits for any U.S. person engaging in a restricted transaction. The rule permits these audits to be conducted internally as long as they are conducted independently. The audit must focus on the U.S. person's restricted transactions and assess relevant materials, such as compliance policies, personnel, and facilities. Audits must verify compliance with security requirements, due diligence measures, and any conditions imposed by the DOJ or applicable licenses.
- **Recordkeeping Obligations:** The rule imposes detailed recordkeeping requirements for U.S. persons engaged in restricted transactions. Businesses must maintain complete and accurate records of each restricted transaction for at least 10 years. Required documentation includes data compliance program policies, audit results, due diligence documentation, and annual certifications, among others.
- **Due Diligence Obligations:** The rule mandates that U.S. persons implement a robust data compliance program to conduct due diligence on restricted transactions. This program must include (1) policies and procedures to identify and mitigate risks associated with cross-border data transfers; (2) assessments of how covered data is transferred, including the types of data involved, the parties to the transaction, and the intended use of the data; and (3) mechanisms to monitor compliance and report violations promptly to the DOJ.
- **Security Obligations:** The rule incorporates CISA Security Requirements to ensure that covered systems and data are protected against unauthorized access and exploitation such as multi-factor authentication and password requirements and approval processes for deploying new hardware or software in covered systems.

5. Exemptions

The rule acknowledges that certain transactions, by their nature, pose minimal national security risks and are therefore exempt from many of the rule's prohibitions, restrictions, and compliance obligations. Examples of exempt transactions include (1) transactions involving personal communications that do not transfer "anything of value"; (2) transfers of commercial or non-commercial information, such as published materials or publicly available research; (3) transactions for official business of the U.S. government; and (4) transactions between a U.S. person and its subsidiary or affiliate located in or directed by a country of concern if they are "ordinarily incident to and part of administrative or ancillary business operations."

6. Enforcement and Penalties

Companies found to violate the rule may face significant penalties, including civil fines and/or criminal liability. The rule imposes a maximum civil penalty of $368,136 or twice the amount of the transaction. The DOJ has emphasized its commitment to strict enforcement to deter unauthorized data transfers,

although the intentions of the Trump Administration to enforce the Final Rule have yet to be seen.

Implications for Businesses

The DOJ's final rule introduces a complex compliance landscape for companies involved in cross-border data transfers, particularly those operating in industries that handle large volumes of sensitive or government-related data. Key considerations for businesses include:

To mitigate risks and ensure compliance, companies should both: (1) conduct a comprehensive review by evaluating existing data transfer practices and identifying any exposure to foreign adversaries and (2) monitor regulatory developments by staying informed about updates to the rule and related regulatory initiatives to ensure ongoing compliance.

Kilpatrick Townsend is closely monitoring these developments and is available to assist clients in navigating the complexities of the DOJ's final rule.