Legal Update Article

DOJ New Data Transfer Rule Impacts Hiring Practices, Business Operations, and Vendor Management: Time to Review Your Privacy + Cybersecurity Program

By Mary T. Costigan

April 28, 2025

Meet the Authors

Mary T. Costigan
Principal
908-795-5135
Mary.Costigan@jacksonlewis.com

Related Services

International Employment
Privacy, Data and Cybersecurity

Takeaways

- The rule prohibits or restricts U.S. companies from making sensitive data available to "countries of concern" or certain persons located in or associated with them.
- The rule applies to hiring practices, vendor engagement, investor due diligence, and data brokerage.
- Enforcement begins 07.08.25.

Related link

- Federal Register: Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons

Article

U.S. organizations should carefully review and ensure their privacy and cybersecurity practices comply with a wide-ranging new federal rule establishing data transfer restrictions regarding sensitive U.S. personal data.

The Department of Justice's (DOJ's)newly operative data transfer ruleprohibits U.S. companies from selling, leasing, or otherwise making sensitive data available to certain third parties located in or associated with six designated "countries of concern": China, including Hong Kong and Macau, Cuba, Iran, North Korea, Russia, and Venezuela. This includes entering into employment, vendor, and investment agreements that will involve access to sensitive data by "covered persons," which is broadly defined and borrows from the Department of the Treasury, Office of Foreign Assets Control's "50 percent rule."

The DOJ rule has the potential to impact companies if they sell, lease, or otherwise make available certain sensitive data to third parties. Businesses in such sectors as life sciences, healthcare, financial services, information technology, higher education, data brokers, and consumer industries appear to have relatively greater exposure to the DOJ rule than others due to the sensitivity of their data and business operations. The rule may also apply as a result of general business practices, regardless of business sector or industry, such as when a company engages an AdTech vendor to collect website user-level data from its website for marketing and advertising related purposes.

Even if a company does not make this data directly available to third parties as part of its operations, the rule may apply if the company maintains the requisite volume of data and its employees, vendors, or investors could access the data incident to their relationship

with the company. To assess whether the rule applies, the company should consider its remote IT and customer service workers, and even board members, and vendors that handle outsourced data processing functions, including IT support or data storage.

Sensitive personal data includes a wide range of data if it is linked or linkable to an identifiable U.S. person. In addition to personal identifiers when they are linked or linkable to other sensitive data (such as a Social Security number linked to a first and last name, an account username linked to a first and last name, and a first and last name linked to an email address and to an IP address), it includes certain human 'omic data, biometric data, health and financial data, and precise geolocation data.

The volume of sensitive data that triggers application of the rule varies based on the nature of the data, as noted in the following chart.

Type of U.S. sensitive personal data	Threshold of data collected about or maintained on…
Human genomic data	100 U.S. persons
Human epigenomic data	1,000 U.S. persons
Human proteomic data	1,000 U.S. persons
Human transcriptomic data	1,000 U.S. persons
Biometric identifiers	1,000 U.S. persons
Precise geolocation data	1,000 U.S. devices
Personal health data	10,000 U.S. persons
Personal financial data	10,000 U.S. persons
Covered personal identifiers	100,000 U.S. persons
Combined data, as described in § 202.205(g)	Lowest applicable number

Companies that collect data within the scope of the rule must demonstrate steps taken to avoid prohibited transfers as well as manage restricted transfers. Compliance requires:

- Implementing robust know-your-data practices;
- Conducting documented due diligence on potential customers, clients, business partners, employees, vendors, and investors to determine their identity;
- Developing a written compliance program;
- Adhering to reporting and recordkeeping requirements; and
- Implementing required security safeguards based on standards issued by the Cybersecurity and Infrastructure Security Agency.

Certain research work or federally funded work may be subject to exemptions.

The rule went into effect on April 8, 2025, and enforcement begins July 8, 2025; organizations have until Oct. 6, 2025, however, to develop compliance programs related to restricted transactions.

Jackson Lewis attorneys are available to assist companies in determining whether and how their business is affected by the rule.