Navigating the DOJ's New Data Transfer Rule: Implications and Compliance Requirements

APRIL 29, 2025

D. REED FREEMAN JR., MAYA S. COHEN, NATALIE TANTISIRIRAT

On January 8, the US Department of Justice (DOJ) issued a final rule under Executive Order 14117, which established the Rule Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons (the Rule).

Read Executive Order 14117 **here**.

The Rule, which took effect on April 8, establishes export-like restrictions and prohibitions on transferring specific types of "bulk U.S. sensitive personal data" and certain specified "government-related data" (including of current or recent US government employees and sensitive government location data) to designated "countries of concern," including China (with Hong Kong and Macau), Iran, North Korea, Cuba, Venezuela, and Russia, as well as transactions involving "covered persons," which includes entities that are established under the laws of by a country of concern and their employees. The Rule established high civil penalties and allows for criminal enforcement. However, on April 11, DOJ paused civil enforcement until July 8 on the express condition of "good-faith" efforts to comply, or to come into compliance with the Rule, in the meantime. Criminal enforcement was not paused.

Who and What Is Covered?

The Rule delineates four main categories of "covered data transactions," which are defined as:

1. Any transaction that involves any access by a country of concern or covered person;
2. To any bulk US sensitive personal data or government-related data; and that involves:
    a. Data brokerages;
    b. Vendor agreements (including those involving cloud services);
    c. Employment agreements; or

d. Investment agreements.

"Sensitive personal data" is classified into seven distinct types, specifically:

1. Covered personal identifiers (e.g., name and contact information, financial account numbers, Social Security Numbers, IP addresses, MAC addresses, device IDs, and Ad IDs);
2. Precise geolocation data (within 1,000 meters);
3. Biometric identifiers;
4. Human 'omic data (i.e., genomic, epigenomic, proteomic, and transcriptomic data);
5. Personal health data (broadly defined);
6. Personal financial data (broadly defined); and
7. Any combination of the above categories.

"Bulk" means any amount of sensitive personal data that meets or exceeds the threshold for the respective "sensitive personal data" at any point in the preceding 12 months, whether through a single covered data transaction or aggregated across covered data transactions involving the same US person and the same foreign person. As seen in the table below, each category of sensitive personal data has a different bulk threshold:

Sensitive Category	**Bulk Threshold**
Human 'omic data	more than 1,000 US persons
Human genomic data	more than 100 US persons
Biometric identifiers	more than 1,000 US persons
Precise geolocation data	more than 1,000 US devices
Personal health data	more than 10,000 US persons
Personal financial data	more than 10,000 US persons
Covered personal identifiers	more than 100,000 US persons
Any combination of the above categories	the lowest number of US persons or US devices in that category of data

A "covered person" under the Rule is:

1. A foreign person that is an entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, that is organized or chartered under the laws of, or has its principal place of business in, a country of concern;
2. A foreign person that is an entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by one or more persons described in points 1, 3, 4, or 5;
3. A foreign person, that is an individual, who is an employee or contractor of a country of concern or of an entity described in points 1, 2, or 5;
4. A foreign person that is an individual, who is primarily a resident in the territorial jurisdiction of a country of concern; or
5. Any person, wherever located, determined by the Attorney General:
    a. To be, to have been, or to be likely to become owned or controlled by or subject to the jurisdiction or direction of a country of concern or covered person.

b. To act, to have acted or purported to act, or to be likely to act for or on behalf of a country of concern or covered person; or

c. To have knowingly caused or directed, or to be likely to knowingly cause or direct a violation of this part.

Corporate subsidiaries are treated as separate entities and are covered persons if they otherwise meet the Rule's definition, while business units of a company are not, even if they are located in a country of concern. The Rule also grants the Attorney General wide discretion to determine whether a person has become a covered person.

The Rule also provides several examples to clarify the scope of "covered person" under the Rule. For example, citizens of a country of concern are exempt if they primarily reside in the United States or a third country unless they are individually designated as a covered person by the Attorney General or are employed by a country of concern or covered person.

Prohibited Transactions

The Rule categorically prohibits certain high-risk transactions, such as "data brokerage" transactions involving covered data with countries of concern or covered persons, and transactions involving access to bulk human-omic data or biospecimens.

Data brokerage is defined as "the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or a vendor agreement, involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data."

The Rule intentionally adopts a broad definition of data brokerage to ensure that "there are no significant loopholes for countries of concern to continue to leverage the data brokerage market as a means of acquiring and exploiting government-related or bulk U.S. sensitive personal data."

DOJ emphasized this point in its **Compliance Guide** published on April 11 explaining that the definition of data brokerage captures "activities that may not be thought of in ordinary parlance as data brokerage [but] may nonetheless constitute data brokerage under the [Rule]." For example:

> A U.S. company maintaining a website or mobile application that contains ads with tracking pixels or software development kits that were knowingly installed or approved for incorporation into the app or website by the U.S. company. That transfer or provision of access to government-related or bulk U.S. sensitive personal data to covered persons or countries of concern could constitute data brokerage and could be a violation of the [Rule.]

While data brokerage transactions with countries of concern or covered persons are prohibited, data brokerage transactions causing covered data to be sent to *other* countries (i.e., not countries of concern) require onward transfer contractual provisions and the reporting of violations to ensure that the covered data is not subsequently transferred to a country of concern.

Restricted Transactions

Other types of data transactions, including those in connection with vendor, employment, and investment agreements, are only "restricted" and therefore permitted under strict conditions. These transactions must adhere to robust **security requirements** developed by the Cybersecurity and Infrastructure Security Agency (CISA), which include organizational and system-level cybersecurity controls, data-level protections like encryption and data minimization, and annual independent audits with detailed recordkeeping. Restricted transactions are also subject to due diligence, audit, recordkeeping, and reporting requirements that mandate the development and implementation of a

written data compliance program no later than October 6.

The Rule also imposes significant record keeping requirements requiring full and accurate records for *any* transaction (not just those that are prohibited or restricted) subject to the Rule to be kept for at least 10 years. There are also heightened record keeping requirements for US persons engaging in restricted transactions (including written policies describing the data compliance program, implementation of the security requirements, results of annual audits, and due diligence conducted to verify the data flow involved in any restricted transaction).

Restricted transactions are limited to data transactions in connection with vendor agreements, employment agreements, and investment agreements, each of which is defined in the Rule and discussed in its accompanying commentary.

Vendor agreements are defined as "any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration." As the definition of vendor agreements is very broad, the Rule provides helpful examples of what constitutes a vendor agreement. Specifically:

- Example 1, involving a country of concern vendor that processes and stores bulk precise geolocation data collected through an app owned by a US company;
- Example 2, involving IT-related services provided by a country of concern vendor to a US medical facility;
- Example 3, involving a country of concerns' vendor providing data centers that provide managed services to US companies; and
- Example 4, involving a US mobile games developer that receives software development services from a country of concern vendor.

A written agreement is *not required by the text of the Rule but* is recommended in order to make the nature of a data transaction between parties clearly within the "vendor agreement" (and thus restricted, rather than prohibited) category, and to be able to respond to a DOJ inquiry.

Employment agreements involve "any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level." In terms of a restricted employment agreement, the Rule describes a situation where a US company hires an individual from a country of concern to perform job functions that involve access to sensitive US data.

Investment agreements are defined as any arrangement where a person gains direct or indirect ownership interests or rights in US real estate or a US legal entity in exchange for payment or other consideration and excludes certain passive investments that do not pose national security risks, such as those with less than 10% voting and equity interest without substantive decision-making rights. An example of a restricted investment agreement is a US company planning to build a data center in a US territory to store bulk personal health data on US persons, with a foreign private equity fund from a country of concern providing capital in exchange for a majority ownership stake.

Restricted Transactions and Compliance Obligations

US entities involved in restricted transactions (i.e., covered data transactions in connection with vendor agreements, employment agreements, or investment agreements) are required to establish risk-based written compliance programs, conduct thorough due diligence on counterparties, including ownership and control checks, maintain detailed records, and complete annual independent audits.

Additionally, US persons must report specific transactions, including rejected prohibited transactions, and maintain comprehensive records of all restricted transactions. In its April 11 supplementary package, including a **press release**, **Compliance Guide**, **FAQs**, and **Implementation and Enforcement Policy**, DOJ emphasized the importance of strict compliance with these procedural aspects of the Rule.

Importantly, DOJ also retains the authority to request information or documents, to require testimony, and to conduct hearings regarding *any act or any transaction* — whether prohibited or restricted under the Rule or not — at any time, underscoring the importance of compliance and detailed recordkeeping. Violations of the Rule can result in severe civil penalties (up to $368,136 per violation, or twice the amount of the transaction at issue, whichever is greater), and criminal penalties including prison sentences of up to 20 years and fines up to $1 million.

While DOJ paused civil enforcement until July 8, the pause is expressly conditioned on "good-faith efforts" to comply, or to come into compliance with the Rule between now and then. To emphasize the serious nature of its expectations during this civil enforcement pause, DOJ spelled out what it means by "good-faith efforts," which includes the following types of activities:

1. Conducting internal reviews of access to sensitive personal data, including whether transactions involving access to such data flows constitutes data brokerage;
2. Reviewing internal datasets and datatypes to determine if they are potentially subject to the Rule (referred to as the "Data Security Program);
3. Renegotiating vendor agreements or negotiating contracts with new vendors;
4. Transferring products and services to new vendors;
5. Conducting due diligence on potential new vendors;
6. Negotiating contractual onward transfer provisions with foreign persons who are the counterparties to data brokerage transactions;
7. Adjusting employee work locations, roles, or responsibilities;
8. Evaluating investments from countries of concern or covered persons;
9. Renegotiating investment agreements with countries of concern or covered persons; and
10. Implementing CISA Security Requirements, including the combination of data-level requirements necessary to preclude covered persons access to regulated data for restricted transactions.

Exemptions

The Rule provides several exemptions for otherwise restricted or prohibited data transactions, including official US government businesses, financial services, corporate group transactions, and certain clinical investigations and regulatory submissions for drugs, biological products, and medical devices. For the purposes of this alert, we will only analyze the financial services and corporate group transactions exemptions.

Financial Services

The exemption for financial services specifically relates to data transactions that are "ordinarily incident to and part of the provision of financial services." These include, for example:

1. Banking, capital markets, or financial insurance services;
2. The transfer of covered data incidental to the purchase and sale of goods and services (such as online shopping or e-commerce marketplaces);
3. The provision or processing of payments or funds transfers (such as services for payment dispute resolution, payor authentication, tokenization, payment gateway, or payment fraud detention); and
4. Provision of investment management services.

The Rule also provides 12 examples for what data transactions may fall within the financial services exemption. One of the examples relates specifically to e-commerce:

> As part of operating an online marketplace for the purchase and sale of goods, a U.S. company, as ordinarily incident to and part of U.S. consumers' purchase of goods on that marketplace, transfers bulk contact information, payment information (e.g., credit-card account number, expiration data, and security code), and delivery address to a merchant in a country of concern. The data transfers are exempt transactions because they involve access by a covered person to bulk personal financial data, but they are ordinarily incident to and part of U.S. consumers' purchase of goods.

As a result, the financial services exemption provides some allowance for online marketplaces and other forms of e-commerce, even where bulk personal financial data is transferred to a country of concern. DOJ should address the full contours of this exemption in future guidance.

Corporate Group Transactions

The corporate group transactions exemption permits otherwise prohibited or restricted data transactions "between a U.S. person and its subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction, or control) of a country concern," where they are *ordinarily incident to and part of the administrative or ancillary business operations*. According to the Rule, such ordinarily incident activities include:

1. Human resources;
2. Payroll, expense monitoring and reimbursement, and other corporate financial activities.
3. Paying business taxes;
4. Obtaining business permits or licenses;
5. Sharing data with auditors or law firms for regulatory compliance;
6. Risk management;
7. Business-related travel;
8. Customer support;
9. Employee benefits; and
10. Employees' internal and external communications.

In the Rule's commentary as well as the FAQs, DOJ clarified that while the administrative and ancillary business are "illustrative and not exhaustive," those exempt activities do not include "core business activities, such as product development and research."

As with other areas of the Rule, these two exemptions are complex and misapplications of them could have serious consequences. When considering them and other aspects of the Rule, consult counsel.

Finally, US persons may also seek specific licenses for otherwise prohibited transactions on a case-by-case basis.

Key Takeaways

The Rule significantly expands US national security controls over sensitive personal data and will affect a broad spectrum of US businesses, particularly in e-commerce, technology, health care, financial services, and cloud computing. While initial compliance costs, such as assessments and remediation, are one-time expenses, businesses will encounter numerous ongoing obligations, including continuous due diligence, compliance program updates, monitoring, regular audits, and detailed recordkeeping and reporting.

Industries such as e-commerce and online advertising, which depend on vast amounts of personal data to enhance customer engagement and optimize marketing strategies, will be significantly affected by the Rule. The broad definition of data brokerage under the Rule has important implications for how these industries manage data transactions. E-commerce businesses may need to reevaluate and update their data management practices, especially as it pertains to third-party vendors and other service providers that may have access to sensitive data.

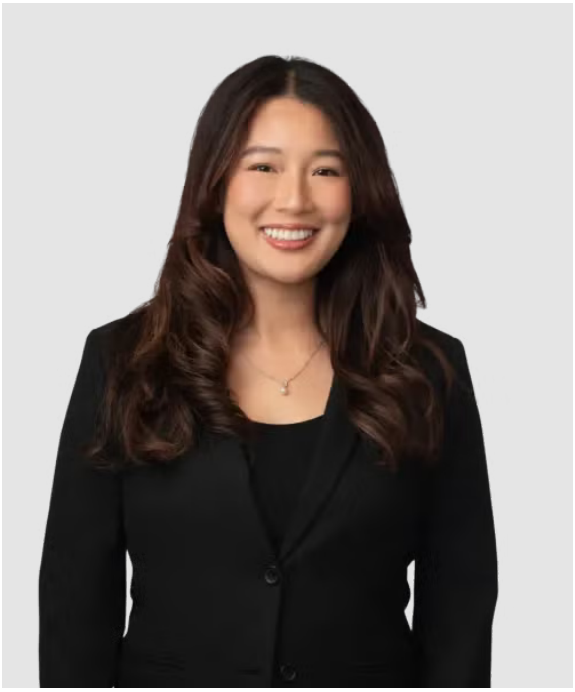
The Rule is detailed and complex, and compliance is time-consuming and resource intensive. Now is the time to consult experienced counsel, take inventory of your data transactions, assess compliance obligations, and engage in the types of "good-faith efforts" enumerated by DOJ and listed above.

If you have questions about how the Rule may affect your business, please reach out to **Reed Freeman Jr.** or another member of the firm's **Privacy, Data Protection & Data Security** practice group.

Contacts

D. Reed Freeman Jr.
PARTNER

Maya S. Cohen
ASSOCIATE



Natalie Tantisirirat
ASSOCIATE

Related Practices

Privacy, Data Protection & Data Security

Continue Reading

ALERTS

Massachusetts Court Expands the Temporal Scope of the Ending Forced Arbitration of Sexual Assault and Sexual Harassment Act

OCTOBER 15, 2025 | LAUREN C. SCHAEFER, KIMIA POURSHADI, NANCY J. PULEO

ALERTS

E-Verify Users Must Restart Using E-Verify and Quickly Catch-Up on Pre-Shutdown Cases.

OCTOBER 13, 2025 | BERIN S. ROMAGNOLO, NANCY A. NOONAN

ALERTS

Court Upholds Pension Reductions Under MPRA, No Taking Found

OCTOBER 10, 2025 | ALISON LIMA ANDERSEN, MARGHERITA A. CAPOLINO

All Insights from Alerts