DORSEY
DORSEY+WHITNEY LLP

Justice Issues Final Rule Restricting Transfer of Personal U.S. Data to Countries of Concern, Effective in April 2025

by Dave Townsend, Austin T. Chambers, Lawrence Ward, T. Augustine Lo, and Justin T. Huff

The U.S. Department of Justice ("DOJ") published its final rule ("Final Rule") on January 8, 2025, that will prohibit or restrict transfer of certain data of U.S. persons to countries of concern, including to China. The Final Rule largely tracks with DOJ's notice of proposed rulemaking ("Proposed Rule"), which we summarized in a previous eUpdate. The Final Rule therefore adopts the basic structure of prohibiting certain data transactions, while permitting restricted transactions only if security requirements are implemented to protect U.S. personal data.

In short, knowing the type of data, the type of transaction, and the location of any person who can access the data is required to determine whether a prohibition or restriction applies to the proposed transaction or transfer of the data under the Final Rule. As explained below, the Final Rule reaches many types of transactions, may cover merely providing access to certain data of U.S. persons, and has a framework of exclusions that may allow companies that would otherwise be regulated by the Final Rule to continue to transfer personal data to countries of concern.

The Final Rule is generally effective starting on April 8, 2025, meaning that data transfers after that date will be subject to the Final Rule and the potential penalties for transactions that violate the Final Rule. DOJ delayed the effective date for certain due diligence and auditing requirements to October 5, 2025. In its discussion of the Final Rule, DOJ rejected delaying the effective date further due to what it describes as the need to quickly address transfers of sensitive U.S. personal data to countries of concern. DOJ also holds open the possibility of delaying the effective date of the Final Rule, either in part or in full, through general licenses or regulatory changes.

This eUpdate summarizes key aspects of the Final Rule, with a particular focus on changes since the Proposed Rule. The eUpdate does not comprehensively describe the Final Rule. In particular, we note our previous summary of the auditing requirements, due diligence, potential penalties, and other details of the Proposed Rule (see link above), most of which are unchanged by the Final Rule.

Related People

- Dave Townsend
- Austin T. Chambers
- Lawrence Ward
- T. Augustine Lo
- Justin T. Huff

Related Capabilities

- National Security Law
- Corporate Governance & Compliance
- Privacy & Social Media

Legal Background

By issuing the Final Rule, DOJ has concluded the rulemaking process to implement Executive Order ("EO") 14117 dated February 28, 2024.

As a basis for regulating international data transfers, EO 14117 and the Final Rule declare an international emergency under the International Emergency Economic Powers Act ("IEEPA"). In particular, President Biden in EO 14117 identified efforts to access and exploit government-related data or bulk U.S. personal data by countries of concern as an unusual and extraordinary threat to U.S. national security. DOJ identifies counterintelligence concerns, the risk of blackmail and ransomware, and the ability to use artificial intelligence ("AI") tools as justifying action under the Final Rule. DOJ also notes a gap in federal law that currently does not address international data transfers to countries of concern.

Who is Impacted by the Final Rule?

The Final Rule broadly applies to and regulates the activities of U.S. companies and individuals operating in many industries and markets. The framework for the Final Rule is outlined below. Initially, however, it is worth highlighting some examples of activities that DOJ believes are subject to the Final Rule, which are indicative both of the scope of and priorities reflected in the Final Rule.

We note these examples with caution, as the status of these examples under the Final Rule could change depending on the precise facts (e.g., amount of data collected), and the activities described below may be permissible if relevant parties adopt security measures, or if the activities qualify for an exemption. We thus refer to these examples as subject to potential restrictions under the Final Rule, depending on the facts and circumstances of the transactions.

- A U.S. company develops mobile app games that collect data on U.S. users. The U.S. company hires a CEO from a country of concern, who will be provided access to data on the U.S. users. The hiring of the CEO is subject to potential restrictions under the Final Rule.
- A U.S. company develops social media apps that systematically collect data of U.S. users. A foreign company from a country of concern purchases a minority stake in the U.S. business. The investment agreement allows the foreign company to access the data of U.S. users. The investment agreement is subject to potential restrictions under the Final Rule.
- A U.S. company operates an app that gathers geolocation data of U.S. users. The U.S. company enters into a vendor agreement with a country of concern to process and store the data. The vendor agreement is subject to potential restrictions under the Final Rule.
- A medical facility with health data about U.S. patients contracts with a company in a country of concern to provide IT-related services, including by providing access to the data about U.S. patients. The contract is subject to potential restrictions under the Final Rule.
- A multinational company maintains data about U.S. persons and contracts with a service provider in a country of concern to process and store the data, including the

data about U.S. persons. The service agreement is subject to potential restrictions under the Final Rule.

- A U.S. company hires a data scientist who is a citizen of a country of concern to develop an AI personal assistant intended for the U.S. company's financial services customers. The data scientist's responsibilities require access to data on large numbers of U.S. persons. The employment of the data scientist is subject to potential restrictions under the Final Rule.

As is apparent from these examples, the Final Rule applies to and potentially restricts the activities of companies in many industries and in a wide range of common IT and business operations. Below we summarize key aspects of the Final Rule.

Key Definitions in Final Rule

The Final Rule applies to U.S. persons who process sensitive U.S. government or bulk U.S. sensitive personal data as described below, and in particular those who engage in transactions with or have operations in countries of concern. However, the Final Rule also will significantly impact non-U.S. persons or operations involving countries other than countries of concern, to the extent they may be involved with U.S. government data or bulk U.S. sensitive personal data and there is or may be potential access to personal data in countries of concern.

DOJ adopts the following key definitions in the Final Rule, all of which are closely aligned with those in the Proposed Rule.

- **"Bulk U.S. Sensitive Personal Data."** The Final Rule adopts "bulk" thresholds consistent with the Proposed Rule. These categories are summarized in the chart at the end of this eUpdate. In a change from the Proposed Rule, DOJ also established a bulk threshold for epigenomic, proteomic, or transcriptomoic data of U.S. persons.
- **"Countries of Concern."** The Final Rule designates six countries—China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela as countries of concern. This list can be expanded upon further designations of countries that pose a risk to U.S. national security.
- **"Covered Person."** The Final Rule prohibits or restricts transfers to a Covered Person in addition to a Country of Concern. DOJ revised the definition of a Covered Person to cover the following: (1) foreign entities that are 50 percent or more owned (individually or in the aggregate) by a Country of Concern, organized under the laws of a Country of Concern, or have their principal place of business in a Country of Concern; (2) foreign entities that are 50 percent or more owned (individually or in the aggregate) by a Covered Person; (3) foreign employees or contractors of countries of concern or entities that are Covered Persons; and (4) foreign individuals primarily resident in Countries of Concern. DOJ also can specifically designate persons, regardless of location, that it determines to be, or to have been, controlled by or under the jurisdiction of a Country of Concern or a Covered Person.
- **"U.S. Person."** A U.S. person includes any individual or entity who is located in the United States; individuals who are U.S. citizens, nationals, or permanent residents, or have refugee or asylee status under U.S. law; and corporations organized solely under the laws of the United States.
- **"U.S. Government Data**." U.S. Government-Related Data includes two types of data, regardless of the volume of the data: (1) geolocation data covering any precise location data within specific longitude and latitude coordinates within areas identified

in the Final Rule; and (2) data about U.S. Government personnel marketed as linked to current or recent former U.S. Government employees or contractors. The Final Rule defines "recent employees or contractors" as those who worked for the U.S. Government (including the military and intelligence community) within a two-year period preceding a covered transaction.

Prohibited, Restricted, and Exempt Transactions

The Final Rule creates a framework of prohibited, restricted, and exempt transactions. Companies will need to consider whether they have transactions of U.S. Government or Bulk Sensitive U.S. Person Data with Countries of Concerns or Covered Persons, and if so, whether those transactions are prohibited, restricted, or exempt. The Final Rule also prohibits facilitating prohibited or restricted transactions, actions taken to circumvent the Final Rule, or causing a violation of the Final Rule.

This framework ultimately will allow certain companies to continue working or collaborating with countries of concern. Companies can rely on the categories of exempt transactions to permit sharing of certain data between the United States and a Country of Concern. Alternatively, certain restricted transactions may, however, proceed if companies adopt security requirements specified in the Cybersecurity and Infrastructure Security Agency ("CISA") rules. The CISA security requirements can be found online and are summarized below.

The Final Rule prohibits U.S. persons from engaging in two types of transactions.

1. **Data Broker Transactions.** The Final Rule prohibits a "Data Brokerage" transaction with a Country of Concern or a Covered Person that involves Bulk U.S. Sensitive Personal Data. A "Data Brokerage" transaction means selling, licensing, or similar commercial transactions where the recipient did not collect or process the data directly from the individuals linked or linkable. By definition, a "Data Brokerage" transaction is not an employment agreement, investment agreement, or vendor agreement as those terms are defined below. These Data Brokerage transactions are defined more broadly than transactions under other data brokerage laws, and the DOJ notes as justification for this broad definition that the operation of ad exchanges, the use of social media, or other "tracking" pixels can allow access to Bulk Sensitive U.S. Personal Data or U.S. Government Data by a Covered Person or in a Country of Concern.
2. **Human Genetic Data.** The Final Rule prohibits a U.S. person from engaging in a transaction with a Country of Concern or a Covered Person involving bulk human genomic data, or data concerning bulk epigenomic, proteomic, or transcriptomoic as defined below at the end of this eUpdate.

The Final Rule makes the following three classes of transaction restricted: (1) employment agreements, (2) non-passive investment agreements, and (3) vendor transactions (collectively, "Restricted Transactions"). Unless the U.S. person adopts CISA's proposed risk mitigation security requirements, U.S. persons cannot engage in the following Restricted Transactions with Countries of Concern or a Covered Person if they involve Bulk U.S. Sensitive Personal Data.

1. **Employment Agreements.** Agreements or arrangements where an individual, other

than an independent contractor, performs work or job functions in exchange for payment or other consideration, including on a board or committee, executive-level arrangements or services, or employment services at an operational plant.
2. **Investment Agreements.** The exchange of payment or other consideration for direct or indirect ownership interests or rights in relation to real estate in the United States or a U.S. legal entity. The Proposed Rule excludes from an "Investment Agreement" passive investments such as for publicly traded securities, index funds, or as a limited partner in a venture capital fund.
3. **Vendor Agreements.** The provision of goods or services, including cloud-computing services, in exchange for payment or other consideration, other than an Employment Agreement.

The Final Rule also establishes a framework of exempt transactions that will make many data processing activities and transactions outside of the Final Rule's prohibitions or restrictions. In particular, the following nine types of activities or transactions may qualify for exemptions under the Final Rule.

1. **Personal communications, informational materials, and travel information** are exempt under the Final Rule. This exclusion recognizes long-standing exclusions, mandated under the IEEPA statute, from IEEPA-based U.S. economic sanctions administered by the U.S. Department of the Treasury Office of Foreign Assets Control ("OFAC"). Companies will need to carefully consider the scope of these exemptions, which DOJ likely will interpret narrowly, similar to OFAC's narrow interpretation of them.
2. Activities involving **U.S. Government** operations.
3. **Financial services** for banking, capital markets, futures or derivatives, or financial insurance services, e-commerce, and certain investment management services.
4. **Corporate group transactions** between a U.S. person and its foreign subsidiary or affiliate, if they are ordinarily incident to and part of routine administrative or business operations, such as human resources, payroll, taxes, permits, compliance, risk management, travel, and customer support.
5. Transactions related to certain **federal law or international agreements**. DOJ cites the following legal instruments as authorizing transactions under this exemption: the Convention on International Civil Aviation (2022); the WHO constitution (1946); various U.S.-China agreements on customs, legal assistance, and taxation; the U.S.-Cuba Extradition Treaty (1905); U.S.-Russia agreements on customs (1994) and legal assistance (1999); the U.S.-Venezuela Legal Assistance Treaty (1997), the International Health Regulations (2005); and certain public health surveillance and response mechanisms.
6. Investment agreements that are subject to mitigation or other action taken by the **Committee on Foreign Investment in the United States ("CFIUS")**, if CFIUS explicitly designates them as exempt.
7. Transactions that are ordinarily incident to and part of the provision of **telecommunications services**, including voice and data communications services regardless of delivery method. DOJ lists communications via cable, Internet Protocol, wireless, fiber, or other transmission mechanisms, as well as arrangements for network interconnection, transport, messaging, routing, or international voice, text, and data roaming as potentially qualifying for this exemption.
8. Transactions involving data transfers or access to data with a Country of Concern or Covered Persons involving **drug, biological product, device, or combination product approvals or authorizations** if such approvals are necessary to obtain or maintain regulatory approval. "Regulatory approval data" means sensitive personal

data that is de-identified or pseudonymized under FDA regulations (21 C.F.R. 314.80(i)) and required by a regulatory entity to research or market a drug, biological product, device, or combination product, including post-marketing studies and surveillance.

9. **Clinical investigations and post-marketing surveillance data** if the transactions are part of clinical investigations regulated by the FDA under sections 505(i) and 520(g) of the Federal Food, Drug, and Cosmetic Act, or to support FDA applications for research or marketing permits for drugs, biological products, devices, combination products, or infant formula, and the data are de-identified or pseudonymized consistent with FDA regulations (21 C.F.R. 314.80(i)).

Final CISA Security Rule

Under the Final Rule, Restricted Transactions may be permitted on the condition that certain security procedures and controls are put in place to protect U.S. Government Data or Bulk Sensitive U.S. Personal Data (collectively, Covered Data). These security controls must be implemented with respect to any "Covered System" that is used to process Covered Data as part of a Restricted Transaction, regardless of whether Covered Data has been deidentified or encrypted on that system. Further, in a clarification in the Final Rule, the existence of security measures does not affect the application of the Final Rule, in principle, meaning that the existence of comparable security controls (e.g. encryption) does not impact companies' obligations to comply with other requirements of the Final Rule.

Under CISA's final security rule requirements, there were relatively few changes to the mandatory security processes and controls relative to the proposed CISA rule. However, certain incremental changes were made, and the final CISA rule allows companies to take a slightly more flexible and risk-based approach with respect to certain controls, in particular those relating to vulnerability management, logging, and certain systems documentation.

As with the Proposed Rule, CISA's security requirements borrow heavily from NIST Cybersecurity Framework and Privacy Framework standards. However, the specificity of these requirements, and CISA's intent to build on the specific national security objectives set out in the Order, mean that these requirements include a number of new and unique obligations for affected organizations. Organizations engaging in Restricted Transactions that must conform to the CISA rules will therefore be required to conduct additional IT system reviews, update applicable policies, and establish additional security controls in order to properly secure Covered Data in Restricted Transactions.

Conclusion

Companies involved in many industries should consider whether the Final Rule requires adoption of new or revised data policies, including companies involved in cloud computing, e-commerce, education, healthcare, financial services, manufacturing, software design, and others. Please contact one of the Dorsey & Whitney attorneys below if you have questions about the Final Rule.

Summary of Bulk U.S. Sensitive Personal Data

	Definition	**"Bulk" Threshold (U.S. persons)**
Biometric Identifiers	Physical characteristics that are measurable or behaviors used to recognize or verify the identity of an individual, including facial, voice, retina or iris, palm, fingerprints, gait, or keyboard usage data that are enrolled in a biometric system and the templates used to create such a system.	1,000
Geolocation	Real-time or historical data that identifies the physical location of an individual or a device with a precision of within 1,000 meters	1,000
Human Genomic	Nucleic acid sequences that are the entire set or a subset of genetic instructions found in human cells, including the result of an individual's genetic test and genetic sequencing data.	100
Other Genetic Data ('omic data)	Epigenomic, proteomic, or transcriptomoic data of individuals	1,000
Personal Financial	Data about an individual's credit, charge, or debit card, or bank account, including purchases and payment history; data in a bank, credit, or other financial statement, including assets, liabilities, debts, or trades in a	10,000

	securities portfolio; or data in a credit report or in a consumer report.	
Personal Health	Health information about past, present, or future physical or mental health or conditions of an individual; healthcare information about an individual or payment information about healthcare.	10,000
Personal Identifiers	Identifiers that in combination with any other listed identifier or other data is linked or linkable to sensitive personal data. This includes names linked to device identifiers, social security numbers, driver's license or other government identification numbers, and many others. The definition excludes certain data (e.g., demographic data linked only to other demographic data).	100,000