KIRKLAND & ELLIS

Kirkland Alert

U.S. Department of Justice Issues Final Rule Restricting Transfers of Sensitive Personal Data

05 February 2025

Executive Summary

On December 27, 2024, the U.S. Department of Justice ("DOJ") released its final rule titled "Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons" (the "Final Rule"). This Final Rule carries out Executive Order ("E.O.") 14117 "Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern," which aims to protect data that the U.S. government has deemed sensitive, including geolocation data and health data, and U.S. government-related data from exploitation by countries with an established record of collecting and using such data to enable hacking, surveillance, scams, blackmail and other malicious activities.

The "countries of concern" under the Final Rule currently consist of China (including Hong Kong and Macao), Cuba, Iran, North Korea, Russia and Venezuela. Broadly, the Final Rule prohibits or restricts "U.S. persons" from engaging in certain data transactions concerning bulk sensitive data and U.S. government-related data with such countries of concern and their "covered persons."

"Bulk" under the Final Rule refers to any amount of sensitive personal data, whether the data is anonymized, pseudonymized, de-identified or encrypted, that exceeds certain thresholds in the aggregate over the preceding 12 months before a "covered data transaction."

The Final Rule was published in the Federal Register on January 8, 2025, and becomes effective 90 days after publication (i.e., April 8, 2025). Further, certain affirmative due diligence and audit requirements for restricted transactions will be phased-in and will not become effective until 270 days after publication in the Federal Register (i.e., October 6, 2025). This *Alert* provides a background to the Final Rule, sets forth the scope of the same, as well as describes its implications for businesses.

Background

The U.S. government has alleged that countries of concern have leveraged access to government-related data or bulk U.S. sensitive personal data to conduct harmful cyber activities and foreign influence campaigns, including the tracking and profiling of U.S. individuals for blackmail and espionage. Further, the U.S. government has alleged that countries of concern have utilized their access to gather intelligence on a broad range of individuals, including activists, academics, journalists, dissenters, political leaders and NGO representatives, to intimidate, suppress political dissent, restrict freedom of expression and carry out other forms of civil liberties infringement. Advances in artificial intelligence ("AI"), big data analysis and computing capabilities have only intensified the risks associated with such data access.

In the Final Rule, the DOJ noted that there is currently no federal law or regulation that specifically prohibits or restricts U.S. individuals from granting access to such data to countries of concern via data brokerage, vendor, employment or investment agreements. The Final Rule therefore is complementary to other U.S. national security regimes, including the CFIUS and ICTS regimes.

Scope of Final Rule

Sensitive Personal Data. The Final Rule regulates six key categories of "sensitive personal data", which consists of: (i) covered personal identifiers, (ii) precise geolocation data; (iii) biometric identifiers; (iv) human 'omic data; (v) personal health data; (vi) personal financial data; or (vi) any combination thereof. We describe each of these key categories below.

Category	*Description*	*Bulk Threshold*
Personal identifiers	Includes names linked to social security numbers, names linked to email addresses and IP addresses,	100,000 U.S. persons.

	government identification numbers and names linked to device identifiers.	
Geolocation data	Includes any data that identifies the physical location of an individual or device within a 1,000-meter precision standard and would include GPS coordinates.	1,000 U.S. devices.
Biometric identifiers	Refers to measurable physical characteristics or behaviors used to recognize or verify the identity of an individual (e.g., facial images, voice prints and patterns, retina and iris scans, palm prints and fingerprints).	1,000 U.S. persons.
Human ‘omic data	Refers to human genomic data and three other types of human ‘omic data (epigenomic, proteomic or transcriptomic).	Human ‘omic data collected about or maintained on more than 1,000 U.S. persons; or Human genomic data collected about or maintained on more than U.S. persons.
Personal health data	Refers to information that indicates, reveals, or describes the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual (e.g., height and weight, vital signs, symptoms, test results, diagnostic or treatment, logs of exercise habits and data on purchase or use of medications).	10,000 U.S. persons.

Personal financial data	Refers to information 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 securities portfolio.	10,000 U.S. persons.

Government-Related Data. The Final Rule also controls "government-related data," which includes geolocation data, regardless of volume, for locations that have been determined to pose a heightened risk of being exploited by a country of concern to reveal insights about locations controlled by the U.S. federal government. Such areas will be enumerated by the Attorney General on the list of specified locations (the "**Government-Related Location Data List**").

The term also includes any sensitive personal data, regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials of the U.S. government.

Prohibitions and Restrictions

Prohibited Transactions. The two categories of prohibited transactions are:

- data brokerage involving access to bulk sensitive data or government-related data by a country of concern or covered person; and
- transactions that involve access by a foreign person to government-related data or bulk U.S. sensitive personal data and that involve data brokerage with any foreign person that is not a covered person unless the foreign person agrees to certain contractual restrictions.

Broadly, data brokerage refers to the sale of data, the licensing of access to data, or any other similar commercial transaction involving the transfer of data where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.

Additionally, the Final Rule specifically prohibits data brokerage and covered data transactions involving access to bulk human 'omic data or human biospecimens from

which such data can be derived.

Restricted Transactions. The three categories of restricted transactions are vendor, employment and investment agreements (though passive investments are excluded):

- **Vendor agreements** refer to any agreement or arrangement where persons provide goods or services to another person, including cloud-computing services, in exchange for payment or other consideration.
- **Employment agreements** refer to 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.
- **Investment agreements** refer to any agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to real estate located in the United States or a U.S. legal entity. However, this category excludes passive investments (e.g., investments into over the counter publicly traded securities or limited partnership investments into private equity or venture capital funds without managerial decisions).

U.S. persons engaging in any restricted transactions are required to develop and implement a data compliance program, as well as conduct certain audits to ensure the effectiveness of applicable security requirements. The compliance program should at the minimum, include the following:

- Risk-based procedures for verifying data flows, including procedures to verify and log, in an auditable manner: (i) types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction; (ii) identity of the transaction parties, including any ownership of entities or citizenship or primary residence of individuals; and (iii) end-use of the data and the method of data transfer;
- Where transactions involve vendors, risk-based procedures for verifying the identity of vendors;
- A written policy describing the data compliance program and that is annually certified; and
- A written policy that describes the implementation of security requirements developed by the Department of Homeland Security's Cybersecurity and Infrastructure Agency ("**CISA**") and that is annually certified. The DOJ notes that CISA is concurrently publishing its security requirements,[1] which include, but are not

limited to, cybersecurity measures such as basic organizational cybersecurity policies and practices, physical and logical access controls, data masking and minimization, encryption and the use of privacy-enhancing techniques.

Covered Persons

As noted above, the countries of concern consist of China (including Hong Kong and Macao), Cuba, Iran, North Korea, Russia and Venezuela. The Final Rule also applies to so-called "covered persons," which refers to a definition more closely aligned with the Department of the Treasury's Office of Foreign Assets Control's ("**OFAC**") 50% rule.

The Final Rule defines four classes of covered persons: (1) foreign entities that are 50% or more owned by foreign governments of 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% or more owned 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.[2]

U.S. Persons

The Final Rule primarily applies to U.S. persons, which it defines as United States citizens, nationals, or lawful permanent residents; relevant individuals admitted to the United States as a refugee; entities organized solely under U.S. law, including foreign branches; as well as any person in the United States.

Non-U.S. persons will also be subject to prohibitions, including causing or conspiring to cause U.S. persons to violate the Final Rule and from engaging in transactions that have the purpose of evading the Final Rule.

Knowledge Standard

Unlike other strict liability regimes (e.g., OFAC-administered economic sanctions), the Final Rule only prohibits and restricts transactions by U.S. persons that "knowingly" participate in such prohibited or restricted transactions. The Final Rule defines "**knowingly**" with reference to "actual knowledge" or "reasonably should have known" standards. To determine what an individual or entity reasonably should have known in

the context of prohibited or restricted transactions, the DOJ stated that it would consider relevant facts and circumstances, including the relative sophistication of the individual or entity at issue, the scale and sensitivity of the data involved and the extent to which the parties to the transaction at issue appear to have been aware of and sought to evade the application of the Final Rule.

Exempt Transactions

The Final Rule also exempts certain classes of data transactions from prohibitions or restrictions if certain requirements are met. Broadly, these are personal communications; information or informational materials involving expressive materials; travel information; official business of the United States government; certain ordinary financial services related information; certain corporate group transactions; transactions required or authorized by federal law or international agreements; investment agreements subject to a CFIUS mitigation agreement; transactions incident to and part of providing telecommunications services; data transactions involving drug, biological product, and medical device regulatory approvals (e.g., consistent with U.S. Food and Drug Administration ("**FDA**") regulations); and other (FDA-regulated) clinical investigations and post-marketing surveillance data.

Implications for Investors and Companies

The Final Rule has far-reaching implications for investors and companies across various sectors, especially those that handle sensitive personal and government-related data. While it does not impose blanket requirements for due diligence, recordkeeping, reporting or compliance, it does create expectations that U.S. businesses and individuals will establish compliance programs, which are tailored to each counterparty's data-related risk profile. The nature of these risk-based compliance strategies can differ based on the nature of the business and data handled, including the size and sophistication of the company, the nature of its products and services, its clientele, and partners, as well as its geographic footprint. In cases of violations, the DOJ will assess the effectiveness of the compliance program during enforcement actions.

As an International Emergency Economic Powers Act ("**IEEPA**")-based program, the Final Rule imposes both criminal and civil penalties. Civil penalties, which are subject to the Federal Civil Penalties Inflation Act, can be up to USD $377,700 or twice the amount of the transaction involved, whichever amount is greater. Next, criminal

penalties apply to any person convicted of willfully committing, willfully attempting to commit, willfully conspiring to commit, or aiding or abetting in the commission of a violation of any license, order, regulation or prohibition issued under IEEPA. Upon conviction, criminal violators may be fined no more than USD $1,000,000, or if a natural person, may be imprisoned for no more than 20 years, or both. DOJ commentary on the Final Rule notes the possibility of submitting voluntary self-disclosures ("**VSD**") about possible violations. The DOJ stated that it intends to publish further guidance and resources on how it would assess VSDs under the Final Rule.

Further, as described above, the Final Rule does set forth express compliance obligations solely for U.S. persons that are involved in restricted transactions. These obligations require the implementation of a thorough compliance program, as well as the requirements to conduct and retain the results of a yearly audit, performed by an independent internal or external auditor, to confirm adherence to security standards set by CISA. Therefore, companies should audit their current universe of data transfer arrangements and agreements, ensuring that they pay special attention to any links to China, as well as other countries of concern.

---

1. CISA has since published applicable security requirements under "*Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117*". ↩

2. These would include Chinese businesses that have access to sensitive U.S. personal data, including Chinese-owned social media enterprises operating in the United States. ↩

Authors

Cori A. Lable, P.C.

Partner / Los Angeles – Century City

John Lynn, P.C.

Partner / Bay Area – San Francisco / Austin

Mario Mancuso, P.C.

Partner / Washington, D.C. / New York

Ivan A. Schlager, P.C.

Partner / Washington, D.C.

Daniel J. Gerkin

Partner / Washington, D.C.

Lucille Hague

Partner / Washington, D.C.

Robert Kantrowitz

Partner / New York

Jodi Wu

Registered Foreign Lawyer (Kirkland & Ellis, Hong Kong) and Partner (Kirkland & Ellis LLP, U.S.) / Hong Kong

Weng Keong Kok

Registered Foreign Lawyer / Hong Kong

Related Services

Practices

- International Trade & National Security
- Cybersecurity & Data Privacy

Suggested Reading

- 06 November 2024 Kirkland Alert Bureau of Industry and Security Proposes Rulemaking Impacting Importation and Sale of Hardware and Software for Connected Vehicles with a Nexus to China and Russia
- 21 October 2024 Kirkland Alert FTC Finalizes “Click to Cancel” Rule Governing Subscriptions and Autorenewals
- 01 October 2024 Kirkland Alert FTC Issues Report and Related Statements on the Use of Consumer Data by Tech Industry