WILMERHALE

DOJ Issues National Security Rule on Sensitive Data Transfers

JANUARY 23, 2025

On January 8, the Department of Justice (DOJ) published its final Rule implementing Executive Order 14117 (EO), "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (the Rule). The Rule establishes a new regulatory regime to be administered and enforced by the Justice Department's National Security Division. Once the Rule is in effect, it will have a significant impact on all US persons engaged in the transfer of sensitive US personal data to "countries of concern" (i.e., China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia and Venezuela).

The Rule identifies certain sensitive data transactions that are prohibited and other transactions subject to special security and reporting requirements. The most notable prohibitions are twofold:

First, the Rule prohibits US persons from engaging in any "data brokerage" transaction involving identified categories of sensitive US personal data with "covered persons" or "countries of concern." Put another way, the Rule bans US data brokers from licensing or otherwise transferring a wide variety of sensitive US persons data to China (among other locations).

Second, the Rule prohibits all US persons from knowingly engaging in any "covered data transaction" with "countries of concern" or "covered persons" involving access to bulk human genomic, epigenomic, proteomic, or transcriptomic data, or with human biospecimens from which such data can be derived.

A broader category of "restricted" transactions—associated with vendor, employment, and investment agreements—condition transfer of certain categories of sensitive US personal data to China and other "countries of concern" on US persons maintaining specified security standards and compliance with government diligence, audit, and reporting requirements.

The Rule is likely to have a widespread impact on many US businesses. Of particular note:

- ***The Rule Will Apply to a Broad Set of US Businesses and Transactions***: The breadth of the Rule means it could have sweeping implications, even for companies that do not typically think of themselves as data brokers.
- ***Sensitive Personal Data is Defined Broadly, with Relatively Low Thresholds***: A broad range of personal data collected in the course of fairly standard online transactions can trigger the Rule. For example, precise geolocation collected by mobile devices, and two or more of the following types of identifiers: device-based or hardware-based identifiers (IMEI, MAC, SIM), advertising identifiers (MAID, Google ad ID), and network-based identifiers (IP address, cookies). The Rule is triggered for such covered personal identifiers at any amount of such data that meets or exceeds 100,000 or more people during a given 12-month period, whether through one covered data transaction or multiple covered data transactions.
- ***Compliance Will Be Challenging***: Entities are expected to focus their efforts on identifying and understanding the data transactions they engage in now in order to comply with the Rule's requirements and prohibitions on sharing bulk US sensitive personal data. In particular, the diligence, auditing, recordkeeping, and reporting requirements for restricted transactions may require that entities either build out or establish comprehensive compliance programs to comply with the Rule.
- ***There is No "Grandfathering" Provision***: Restricted and prohibited transactions will not be grandfathered as compliant simply because any resulting covered data transactions are subject to a preexisting contract or agreement. The DOJ has indicated that businesses that believe compliance is not feasible because of existing obligations may seek a license authorizing otherwise prohibited or restricted transactions. The Rule also empowers DOJ to issue general licenses in its discretion.
- ***The Trump Administration Might Keep the Rule***: Biden's EO 14117 was not one of the many initial recissions made by President Trump on January 20, 2025, his first day in office. The Rule was designed to be narrowly tailored, but also flexible. The focus of the Rule on China and national security appears to be consistent with other protectionist measures likely to be favored by the new administration. Indeed, it is possible the new administration may add additional countries of concern or additional categories of data through supplemental rulemaking.

The Rule is effective April 8, 2025 (90 days after the date of publication in the Federal Register). (However, the Rule is also subject to President Trump's executive order on a regulatory freeze pending review by a new agency leader.) Certain affirmative compliance obligations will be phased in with a later effective date of October 6, 2025 (270 days after the Rule's publication in the Federal Register).

Key Definitions

The Rule captures a substantial range of economic activity with coverage potentially triggered through licensing, joint ventures, investments, employment and vendor agreements, and other transactions resulting in access to certain carefully defined categories of sensitive personal data associated with US persons.

"Country of Concern" and "Covered Person"

The Rule imposes limitations and prohibitions on the ability of "US persons"—defined as US citizens, entities organized under the laws of the US, and individuals lawfully resident in the US—to engage in certain data transfer transactions with "countries of concern" or "covered persons."

The Rule identifies six "countries of concern": China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia and Venezuela.

"Covered persons" are effectively entities and individuals with a substantial nexus to a country of concern. Specifically, "covered persons" are:

(1) foreign persons that are 50 percent or more owned 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) a foreign person that is 50 percent or more owned by a covered person;

(3) a foreign person who is an employee or contractor of countries of concern or entities that are covered persons;

(4) foreign persons primarily resident in countries of concern; or

(5) a foreign person specially designated by the Attorney General of the United States as a covered person.

In light of the authority of the Attorney General to designate specific persons as "covered persons," regardless of location, the Rule essentially creates a sanctions-type list for covered transactions in the future. To determine whether an entity is controlled or subject to the influence of a country of concern, the DOJ will determine whether an entity is subject to the direction or control of a country of concern or covered person and, if so, will publicly designate them as a covered person (§ 202.211(a)(1) through (4)). Accordingly, US companies can rely on the published Covered Persons List when conducting due diligence.

"Covered Data" and "Bulk US Sensitive Personal Data"

Under the Rule, "covered data" includes a broad range of personal data that many companies collect in the ordinary course of doing business. Specifically, it includes the following types of data:

- "Covered personal identifiers" are "any listed identifier: (1) In combination with any other listed identifier; or (2) In combination with other data that is disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data."

- This includes “specifically listed classes of personally identifiable data that are reasonably linked to an individual” and could be used to identify an individual, but excludes (1) demographic or contact data that is linked only to other demographic or contact data (such as first and last name, birthplace, ZIP code, residential street or postal address, phone number, and email address and similar public account identifiers); and (2) a network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifier, account-authentication data, or call detail data as necessary for the provision of telecommunications, networking, or similar.

– “Listed identifier” means any piece of data in any of the following data fields:
  - Full or truncated government identification or account number (such as a Social Security number, driver’s license or State identification number, passport number, or Alien Registration Number);
  - Full financial account numbers or personal identification numbers associated with a financial institution or financial services company;
  - Device-based or hardware-based identifier (such as International Mobile Equipment Identity (IMEI), Media Access Control (MAC) address, or Subscriber Identity Module (SIM) card number);
  - Demographic or contact data (such as first and last name, birth date, birthplace, ZIP code, residential street or postal address, phone number, email address, or similar public account identifiers);
  - Advertising identifier (such as Google Advertising ID, Apple ID for Advertisers, or other mobile advertising ID (MAID));
  - Account-authentication data (such as account username, account password, or an answer to security questions);
  - Network-based identifier (such as Internet Protocol (IP) address or cookie data); or
  - Call-detail data (such as Customer Proprietary Network Information (CPNI).
– “Precise geolocation data” is data, whether real-time or historical, that identifies the physical location of an individual or a device with a precision of within 1,000 meters. Examples of “precise geolocation data” include GPS coordinates and IP address geolocation.
– “Biometric Identifiers” are measurable physical characteristics or behaviors used to recognize or verify the identity of an individual, including facial images, voice prints and patterns.
– “Human ‘omic data” is human genomic data representing nucleic acid sequences and certain other ‘omic data which examines biological processes that contribute to the form and function of cells and tissues.
– “Personal health data” is health 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.

- "Personal financial data" is data about an individual's credit, charge, or debit card, or bank account, including purchases and payment history; data, including assets liabilities debts, and transactions in a bank, credit, or other financial statement; or data in a credit report or in a "consumer report."

The Rule excludes certain categories of data from the scope of the term "sensitive personal data," such as public or nonpublic data that do not relate to an individual (e.g., trade secrets and proprietary information), data that is already lawfully publicly available from government records (such as court records) or widely distributed media, personal communications and certain informational materials, including metadata associated with expressive materials (e.g., geolocation data embedded in digital photographs).

The term "bulk US sensitive personal data" means a collection or set of sensitive personal data relating to US persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted, 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 or covered person, where such data meets or exceeds the following applicable threshold[s]:

- Human 'omic data: 1,000 US persons, or, in the case of human genomic data, more than 100 US persons.
- Biometric identifiers and precise geolocation data: More than 1,000 US persons.
- Personal health data and personal financial data: More than 10,000 US persons.
- Covered personal identifiers: More than 100,000 US persons.
- Any combination of these data types.

"Government-Related Data"

The Rule creates a variety of strict restrictions on the transfer of "government-related data," which is defined as:

- Any volume of precise geolocation data for geographic areas identified by longitude and latitude in an appendix to the Rule (the appendix currently includes 736 such geographic locations); and
- 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 United States Government, including the military and Intelligence Community.

"Covered Data Transactions"

The Rule defines a "covered data transaction" as any transaction involving any access by a country of concern or covered persons to any government-related data or bulk US sensitive personal data and that involves:

(1) data brokerage;

(2) a vendor agreement;

(3) an employment agreement; or

(4) an investment agreement.

The Rule includes illustrative examples of covered data transactions for US entities engaging with a vendor, such as: "[a] US person engages in a vendor agreement with a covered person involving access to bulk US sensitive personal data. The vendor agreement is a restricted transaction. To comply with the relevant security requirements, the US person, among other things, uses data-level requirements to mitigate the risk that the covered person could access the data. The vendor agreement remains a covered data transaction subject to the requirements of this part." The Rule clarifies that US persons or entities engaging with a vendor who is a covered person, but who already has possession of bulk US sensitive personal data, would not be considered a covered data transaction "because the transaction does not involve access by the covered person."

Prohibited Transactions

The Rule establishes five categories of prohibited transactions.

1. "Data Brokerage" with Countries of Concern

The Rule prohibits US persons from knowingly engaging in a covered data transaction involving data brokerage with a country of concern or "covered person."

The Rule defines "data brokerage" to mean "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."

2. Human Genomic (and other 'omic) Data or Human Biospecimens

The Rule prohibits US persons from knowingly engaging in any data brokerage and covered data transactions with countries of concern or covered persons involving access to bulk human "'omic data" (i.e., human genomic, epigenomic, proteomic, or transcriptomic data) or human biospecimens from which such data can be derived.

3. Knowingly Directing a Transaction Out of Compliance with the Rule

The Rule prohibits any US person (wherever located) from knowingly directing any covered data transaction that would be a prohibited transaction or restricted transaction if the transaction would violate the Rule if carried out by a US person. This prohibition applies to transactions even if the transferor is not otherwise subject to the Rule.

4. US Persons Engaging in any Data Brokerage or Government-Related Data Transaction without Contractual Restrictions

The Rule prohibits any US person from knowingly engaging in any transaction that involves any access by a foreign person to government-related data or bulk US sensitive personal data *and* that involves data brokerage with any foreign person that is not a covered person unless the US person:

- "Contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving data brokerage of the same data with a country of concern or covered person"; and
- "Reports any known or suspected violations of this contractual requirement."

Put another way, the Rule requires US persons engaged in data brokerage with any foreign person to satisfy certain conditions, including, but not limited to, contractually requiring that the foreign person refrain from reselling or providing access to that data to a country of concern or covered person through a subsequent covered data transaction. The DOJ has indicated that it anticipates that forthcoming compliance and enforcement guidance will provide model contractual language to satisfy this requirement. The Rule also clarifies that US persons providing third-party platforms or infrastructure are not civilly or criminally responsible for their customers' prohibited or restricted transactions on those platforms. They are only responsible for the prohibited or restricted transactions which they themselves conduct.

5. Evasion Activities and Conspiracies

The Rule prohibits efforts to improperly evade the restrictions set out in the Rule or enter a conspiracy to do so.

Restricted Transactions

Under the new Rule, any "covered data transaction" that occurs through a vendor agreement, employment agreement, or investment agreement, and that involves transfer to countries of concern or covered persons, may only be pursued if the applicable US person complies with a set of specially prescribed security rules and compliance requirements. Of note, however, the restricted transaction provisions of the Rule are not available to data transactions involving so-called 'omic

data transactions with covered persons and countries of concern. Such transactions are not permissible even in the context of an employment, vendor, or investment agreement.

The minimum security rules applicable to restricted transactions were published separately by Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) (CISA Security Requirements). They impose conditions specifically on the covered data that may be accessed as part of a restricted transaction; on the covered systems, more broadly; and on the organization as a whole. The organizational and system-level requirements include ensuring basic cybersecurity policies, practices, and requirements are in place, including remediation of known vulnerabilities, documentation of vendor agreements, data and network mapping, logical and physical access controls, MFA on all covered systems, logging, and identity management. The data-level requirements involve implementation of a combination of mitigations that are sufficient to fully and effectively prevent access to covered data, including data minimization and data masking strategies, encryption techniques, and the use of privacy enhancing technologies.

Exceptions

The Rule includes a variety of important exceptions. Of note:

- *Personal communications / Expressive Information / Travel Information*: The Rule does not capture personal data transactions associated with communications that do not transfer anything of value; the import or export of informational materials involving expressive materials; or travel information, including data about personal baggage, living expenses, and travel arrangements.
- *Financial Services*: The Rule does not capture data transactions ordinarily incident to the provision of financial services, such as certain banking transactions.
- *Government Transactions*: The Rule does not capture data transactions associated with official US government business carried out by agencies, government personnel, or contractors.
- *CFIUS Mitigation*: Investment agreements subject to a mitigation measure agreed to or otherwise imposed by the Committee on Foreign Investment in the United States (CFIUS) are not subject to the Rule.
- *Internal Corporate Transactions*: The Rule does not capture common internal corporate transactions incident to payroll, human resources, company travel, and similar activities.
- *Telecommunications Services*: The Rule does not capture data transactions incident to the provision of telecommunications services.
- *Life Science Authorizations*: The Rule does not capture data transactions associated with drug, biological products, and medical device regulatory approval data. Specifically, the Rule generally does not apply to data transactions that involve "regulatory approval data" that "is necessary to obtain or maintain regulatory authorization or approval to research or market a drug, biological product, device, or a combination product, provided that the US

person complies" with specific recordkeeping and reporting requirements set forth in the Rule.

Regulatory approval data, in this context, means: "sensitive personal data that is de-identified or pseudonymized consistent with the standards of 21 CFR 314.80 and that is required to be submitted to a regulatory entity, or is required by a regulatory entity to be submitted to a covered person, to obtain or maintain authorization or approval to research or market a drug, biological product, device, or combination product, including in relation to post-marketing studies and post-marketing product surveillance activities, and supplemental product applications for additional uses. The term excludes sensitive personal data not reasonably necessary for a regulatory entity to assess the safety and effectiveness of the drug, biological product, device, or combination product."

The Rule also permits the DOJ to issue licenses to authorize categories of otherwise prohibited or restricted transactions under specified conditions. The DOJ intends to issue separate instructions on how to apply for a specific license.

Affirmative Compliance Obligations / Audits / Reporting

The Rule prescribes compliance based on individualized risk profiles. Through this risk-based lens, compliance programs may vary depending on a range of factors such as the company's size, products and services, customers and counterparties, and geographic locations.

Companies engaging in restrictive transactions are obligated to implement a comprehensive compliance program, which includes risk-based procedures for verifying data flows, including procedures to verify and log the types and volumes of data involved, the identities of transaction parties, and the end-use of the data and transfer method. This information must be verified and logged in an auditable manner. The company must also maintain a (i) written policy that describes the compliance program and (ii) a written policy the describes the company's implementation of the CISA Security Requirements and certify the documents annually via the company's compliance officer. If a violation occurs, the DOJ will consider the adequacy of the compliance program in any enforcement action.

Further, companies are obligated to establish written policies on data security and compliance that are certified annually by a responsible officer or employee, conducting and retaining the results of an annual audit by an internal or external independent auditor to verify compliance with the CISA Security Requirements. The auditor must produce a written report describing the following—(i) the nature of the restricted transactions, (ii) the auditor's methodology (including documents reviewed, personnel interviewed, and facilities, equipment, network or systems examined), (iii) the effectiveness of the data compliance program, (iv) the vulnerabilities or deficiencies in the company's implementation of the CISA Security Requirements that have or could increase the risk of access to government-related data or bulk US sensitive data or personal data by a country of

concern, and (v) any instances in which the security requirements failed or were not effective in mitigating the risk of access—and recommend any improvements to policies or practices to ensure compliance with the CISA Security Requirements. The scope of the audit provision was revised to clarify that (i) the US persons may use either internal or external audits so long as they are independent and (ii) the audit report need only address the nature of a US person's restricted transactions.

The Rule also requires certain reporting requirements, including:

- annual reports by any US person engaged in a restricted transaction involving cloud-computing services, if they are 25 percent or more owned, directly or indirectly, by a country of concern or covered person;
- timely reporting of a rejected transaction to curtail attempts to access government-related data of bulk US sensitive personal data. Any US person that has received and affirmatively rejected an offer from another person to engage in a prohibited transaction must submit a report to the DOJ within 14 business days of rejecting it;
- reports for US persons engaged in a covered data transaction involving data brokerage with a foreign non-covered person if the US person knows or suspects that the foreign counterparty is violating the restrictions on resale and onward transfer to countries of concern or covered persons; and
- reports by US persons invoking the exemption for certain data transactions that are necessary to obtain or maintain regulatory approval to market a drug, biological product, device, or a combination product in a country of concern.

The DOJ may—at any time—require an entity to furnish a report or information relative to any act or transaction or covered data transaction, which must be furnished under oath. The Rule outlines the DOJ's authority to conduct investigations, subpoena and examine witnesses, and hold hearings.

To carry out these new requirements, the National Security Division has requested over 45 new positions dedicated to national security programs according to its FY 2025 Budget Request At A Glance.

Consequences of Non-Compliance and Penalties

Violations of the Rule may lead to civil or criminal penalties. The Rule includes a process for imposing civil monetary penalties similar to those used in contexts implicating the International Emergency Economics Powers Act (IEEPA). The maximum civil monetary penalty for violations is the greater of $368,136 or an amount that is twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed. Willful violations can trigger criminal

liability under IEEPA, which can result in fines up to $1,000,000 or imprisonment for 20 years, or both.

Conclusion

This Rule will have broad implications for many U.S. businesses. The Rule marks the creation of a new regulator of cross-border data transactions at the Department of Justice and will require all companies engaged in cross-border data flows to evaluate application of the Rule to their transactions. In addition to transaction diligence, the Rule will also create new cybersecurity standards and reporting requirements for U.S. businesses engaged in restricted transactions.

Contributors

Kirk Nahra
PARTNER

kirk.nahra@wilmerhale.com
+1 202 663 6128

Jason C. Chipman
PARTNER

jason.chipman@wilmerhale.com
+1 202 663 6195

Arianna Evers
PARTNER

arianna.evers@wilmerhale.com
+1 202 663 6122

Ali A. Jessani
COUNSEL

ali.jessani@wilmerhale.com
+1 202 663 6105

Sarah Litwin
ASSOCIATE

sarah.litwin@wilmerhale.com
+1 617 526 6288