National Security Update: DOJ Unveils Rules Restricting Sensitive Bulk Data Transfers

January 10, 2025

DOJ Issues Landmark Rules on Sensitive Data

On December 27, 2024, the U.S. Department of Justice ("DOJ") issued the "Final Rule on Preventing Access to Sensitive Data," creating a comprehensive export control regime to restrict the transfer of bulk sensitive personal and government-related data to foreign adversaries deemed threats to U.S. national security.[1] The rule focuses on protecting critical datasets, including biometric identifiers, health records, genomic data, financial information and precise geolocation data, as outlined in the "Government-Related Location Data List."[2] DOJ emphasized that foreign adversaries could exploit such data for espionage, cyberattacks, malign influence and coercion.

To underscore these risks, DOJ cited real-world cases of unregulated access to sensitive data. Investigators demonstrated vulnerabilities by purchasing digital advertising data from brokers to track U.S. military contractors and soldiers at high-security sites in Germany, exposing entry points, routines and security weaknesses.[3] Similarly, journalists uncovered that a fitness app used by bodyguards of high-profile leaders, including President Biden, revealed precise movements, underscoring how unrestricted access to such data can threaten national security.[4]

---

1 In February 2024, President Biden, pursuant to the International Emergency Economic Powers Act ("IEEPA") issued Executive Order 14117, titled "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government Related Data by Countries of Concern." E.O. 14117 authorizes the Attorney General, in coordination with the heads of other relevant agencies, to issue regulations to prevent the transfer or sale of bulk sensitive personal and government-related data to countries of concern when access would pose an "unacceptable risk to the national security of the United States." This rule implements E.O. 14117.

2 28 C.F.R. Part 202.1401 (2024).

3 Dhruv Mehrotra & Dell Cameron, *Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany*, WIRED (Nov. 19, 2024), https://www.wired.com/story/phone-data-ussoldiers-spies-nuclear-germany/ [https://perma.cc/P5H6-3DFB].

4 Sylvie Corbet, *Fitness App Strava Gives Away Location of Biden, Trump and Other Leaders, French Newspaper Says, Associated Press* (Oct. 28, 2024), https://apnews.com/article/biden-trump-macronbodyguards-security-strava-0a48afca09c7aa74d703e72833dcaf72 [https://perma.cc/W59P-Y6TY].

DOJ also raised significant concerns about human genomic data, warning that adversaries could exploit it to develop bioweapons tailored to specific genetic profiles. Genomic data may reveal critical traits such as health, mental capacity and physical abilities, posing grave risks in intelligence recruitment and military strategy. DOJ cautioned that even anonymized data presents significant threats, as adversaries can analyze patterns of life, identify vulnerabilities within populations and extract broader insights for exploitation.

Current legislative and regulatory frameworks failed to fully address these potential vulnerabilities. Existing laws, such as the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFAA), CFIUS authorities and earlier executive orders,[5] focus on transaction-specific reviews or sector-specific controls but lack broad restrictions on data transactions. The new rule fills this gap by restricting certain sensitive bulk data transactions with countries of concern and covered persons, establishing a process for DOJ's National Security Division ("NSD") to issue licenses for such transfers, provide advisory opinions and enforce specific security mitigation requirements and exemptions. The rule goes into effect in 90 days, with certain portions gradually rolled out over 270 days.

Overview of the Rule's Requirements

The rule prohibits any U.S. individual or entity ("U.S. person") from knowingly engaging in a covered data transaction with a country of concern or a covered person.

- **Covered Persons:** Includes foreign entities 50% or more owned by countries of concern, those organized or operating in such countries, individuals employed by or residing in countries of concern, and individuals designated by the Attorney General as acting on behalf of or directed by a country of concern.

- **Countries of Concern:** Identified as China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela by the Attorney General, with concurrence by the State Department and Department of Commerce, due to their adverse activities against U.S. national security.

[5] The order expands upon the national emergency declared in Executive Order 13873 of May 15, 2019, which focused on securing the information and communications technology and services supply chain. The Commerce Department issues final determinations based these kinds of national security concerns. It also builds on measures from Executive Order 14034 of June 9, 2021, aimed at protecting Americans' sensitive data from foreign adversaries.

The rule has two categories of transactions: prohibited transactions and restricted transactions.

Prohibited Transactions

The two categories of prohibited transactions are data brokerage and covered data transactions involving access to bulk human 'omic data or human biospecimens from which such data can be derived. These transactions are deemed to pose an unacceptable risk to national security and are banned outright.

Restricted Transactions

The three categories of restricted transactions are vendor, employment and nonpassive investment agreements. Restricted transactions may proceed if specific security requirements designed to mitigate risks are met. These requirements, outlined by the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency ("CISA"), include organizational and system-level measures such as asset management, vendor management and access controls and data-level measures such as data minimization, encryption and the implementation of privacy-enhancing technologies. However, this exemption does not apply to bulk human 'omic data or human biospecimens from which such data can be derived.

Data Restricted by the Rule

The rule applies to six categories of U.S. sensitive data sources regardless of whether the data is anonymized, pseudonymized, de-identified or encrypted at various numeric thresholds, including:

- **Precise Geolocation Data:** Data identifying the physical location of an individual or device within 1,000 meters on over 1,000 devices.
- **Biometric Identifiers:** Measurable physical or behavioral characteristics used for identity recognition, such as facial images, voice prints, fingerprints and iris scans. The restrictions go into effect when transfers of such data involve more than 1,000 U.S. persons.
- **Personal Health Data:** Information related to an individual's physical or mental health, healthcare services or associated payments. The restrictions go into effect when transfers of such data involve more than 10,000 U.S. persons.
- **Personal Financial Data:** Information about financial accounts, credit card transactions, trades in a securities portfolio, credit histories and consumer reports.

The restrictions go into effect when transfers of such data involve more than 10,000 U.S. persons.

- **Covered Personal Identifiers:** Personally identifiable data such as Social Security numbers, driver's license numbers, financial account numbers, device identifiers and contact information. The restrictions go into effect when transfers of such data involve more than 100,000 U.S. persons.

- **Human Genome-Related Data:** Sensitive personal data that involves bulk human 'omic data or human biospecimens from which bulk human 'omic data could be derived. This includes data covering genetic, epigenetic, proteomic and transcriptomic analyses of the human genome. For human genomic data, the restrictions go into effect when the data involves over 100 U.S. persons and for the three other categories over 1,000 U.S. persons.

Any volume of sensitive personal data that meets or exceeds the established thresholds within the preceding 12 months—whether from a single covered data transaction or through aggregation across multiple covered data transactions involving the same U.S. person and the same foreign entity or covered individual—qualifies. The data is also restricted to any combination of these data types that satisfies the lowest threshold for any category within the dataset during the 12-month period. In addition, the rule places no threshold amount on the following kinds of data:

- **Government-Related Data:** Includes precise geolocation data and sensitive personal data linked to U.S. government employees, contractors or senior officials, especially those in the military and intelligence sectors. This includes high-risk federal locations designated in the Government-Related Location Data List.

Exemptions

The rule includes nuanced exemptions for specific transactions, including personal communications without exchange of value, transfers of information or informational materials, official U.S. government activities, routine banking and investment financial services, transactions within a U.S. company and its foreign subsidiaries and transactions required by federal law or international agreements.

Third-Party Contractual and Compliance Obligations

The rule prohibits data brokerage with any foreign person who is not a covered person unless the U.S. person ensures contractually that the foreign person will not engage in subsequent covered data transactions with a country of concern or covered person. DOJ expects U.S. persons to develop compliance programs tailored to their risk profiles, including conducting due diligence, performing periodic reviews with foreign

counterparties, implementing robust data security policies, conducting regular audits and maintaining detailed record-keeping practices. Additionally, U.S. persons are required to report any violations or suspected violations of the rule within 14 days of receiving notice.

NSD Licensing Process

The rule establishes a structured process for obtaining licenses to authorize otherwise prohibited or restricted transactions involving sensitive data. There are two types of licenses: general and specific. General licenses apply to a broad class of transactions and are not tied to specific individuals or entities. These licenses are published in the Federal Register, making them available for use by all relevant parties. However, DOJ anticipates that these general licenses will be rare.

Specific licenses are tailored to particular transactions and granted through a formal application process. To obtain a specific license, applicants must submit a detailed application that includes information about the transaction, details of the sensitive data involved, identification of all parties, ownership details, data transfer methods and the intended use of the data. Applications must be submitted electronically to NSD's Foreign Investment Review Section. In some cases, DOJ may request additional information or oral presentations.

To make its determination, DOJ may consult with other relevant agencies, including the State Department, the Department of Homeland Security and the Department of Commerce. Based on this review, DOJ may issue, modify or deny the license. Once the decision is finalized, DOJ will communicate its determination, which constitutes final agency action. DOJ aims to respond to license requests within 45 days of receiving the application and any required supplemental information or documents.

If approved, the license authorizes only the specific transaction described in the application and mandates compliance with all stipulated conditions, such as filing required reports. Noncompliance may result in enforcement action. If a license application is denied, applicants can request reconsideration by providing new information or evidence of changed circumstances.

Advisory Opinions

NSD will issue advisory opinions regarding this rule. Any U.S. person involved in transactions subject to the rule may request an advisory opinion from the Attorney General by submitting it to NSD. Requests must pertain to actual, disclosed transactions and be submitted by a U.S. party or their agent. Requests should not involve

nonparticipating parties. The request cannot be anonymized and must concern prospective conduct and include the identities of the transaction parties, ownership or citizenship details, a description of the transaction (including the nature, volume and end-use of sensitive data) and any potential basis for exemptions. DOJ may request additional information during the review process.

After reviewing the request, DOJ may state its enforcement intentions regarding the proposed conduct, decline to comment or take other necessary actions. DOJ aims to respond to these requests within 30 days after receiving all necessary information. It also reserves the right to amend or revoke these opinions, providing notice of changes through the Federal Register or other means. Any notice of amendment or revocation will include details on when reliance on the previous opinion becomes unreasonable and outline applicable transition periods, when possible.

Penalties

Under IEEPA, the maximum civil penalty is the greater of $368,136 or twice the amount of the violating transaction. Criminal violations may result in fines up to $1,000,000, imprisonment for up to 20 years, or both. If DOJ determines a civil penalty is warranted, it will issue a pre-penalty notice, allowing the alleged violator to respond. After reviewing the response, DOJ may issue a penalty notice, which constitutes a final agency action. Alleged violators may seek additional judicial review in federal district court.

The Final Rule takes effect 90 days after publication in the Federal Register, which is expected for January 8, 2025, although certain compliance requirements will not take effect until 270 days following publication. U.S. companies, universities, institutions and individuals should consider taking the following steps:

- **Understanding Data Flows:** Compliance may be challenging unless U.S. persons understand their data flows—both in terms of volume and type of data but also in terms of the geographic flows of such data. Engaging in data-mapping exercises may alleviate this burden.

- **Updating Contracts:** Updating standard contractual provisions in Data Protection Addenda to ensure onward transfers of any sensitive data are sufficiently restricted consistent with the rule.

- **Gap Assessments:** CISA's security requirements may be onerous for some U.S. persons, and conducting a gap assessment to identify any needed security uplifts can help ensure vendor, employment and nonpassive investment agreements involving data transfers can proceed legally.

- **Licensing:** Assessing whether to seek general or specific licenses for ongoing or otherwise business critical data transfers to ensure sufficient time to obtain such licenses where needed.

* * *

Please do not hesitate to contact us with any questions.

Luke Dembosky
Partner, Washington, D.C.
Tel: +1 202 383 8020
ldembosky@debevoise.com

Rick Sofield
Partner, Washington, D.C.
Tel: +1 202 383 8054
rcsofield@debevoise.com

Carter Burwell
Counsel, Washington, D.C.
Tel: +1 202 383 8149
cburwell@debevoise.com

Robert T. Dura
Counsel, Washington, D.C.
Tel: +1 202 383 8247
rdura@debevoise.com

Johanna N. Skrzypczyk
Counsel, New York
Tel: +1 212 909 6291
jnskrzypczyk@debevoise.com

Emily Kennedy
Associate, Washington, D.C.
Tel: +1 202 383 8112
eakennedy@debevoise.com