King & Spalding

# Client Alert

Special Matters & Government Investigations

JANUARY 07, 2025

# DOJ Issues Final Rule Restricting Foreign Access to U.S. Data

## The rule imposes substantial new diligence, reporting, cybersecurity, and auditing obligations on companies.


*For more information, contact:*

Sumon Dantiki
+1 202 626 5591
sdantiki@kslaw.com

Robert K. Hur
+1 202 383 8969
rhur@kslaw.com

J. Philip Ludvigson
+1 202 626 9267
pludvigson@kslaw.com

Jacqueline Van De Velde
+1 404 572 2450
jvandevelde@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Suite 900
Washington, D.C. 20006
T. +1 202 737 0500

Atlanta
1180 Peachtree Street, NE
Suite 1600
Atlanta, Georgia 30309
T. +1 404 572 4600


On December 27, 2024, the U.S. Department of Justice ("DOJ") issued a final rule implementing Executive Order ("EO") 14117 titled "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." The final rule, which becomes effective 90 days after publication in the Federal Register, imposes due diligence, reporting, and auditing requirements that are expected to take effect in late 2025. The rule will permit DOJ to investigate potential violations and establishes significant civil and criminal penalties for violators.

The final rule will afford the incoming Trump administration a new and significant avenue to address national security risks related to China. It is expected to be vigorously enforced. Companies that engage in bulk data transactions—for example, social media, e-commerce and electronic payment platforms; data marketplaces and aggregators, healthcare and insurance providers; biotechnology companies; and the employees, vendors, and other third parties with whom companies in such industries do business—should be aware of what the rule requires and begin developing an effective compliance program that takes into account due diligence, reporting, and auditing requirements.

### THE EXECUTIVE ORDER

In February 2024, President Biden signed EO 14117, which aimed to address national security threats posed by access to and exploitation of Americans' bulk sensitive personal data and U.S. government-related data. The EO recognized that "countries of concern" can use such data

for cyber-attacks, blackmail, espionage, intimidation, military purposes, and other malicious activities. Tools such as artificial intelligence and high-performance computing enable actors tied to those countries to more effectively manipulate and exploit that data for nefarious purposes.

Accordingly, the EO set out to restrict mass sensitive data transfer, to include data access, to countries of concern and individuals who might be leveraged by those countries ("covered persons").

To implement the EO, President Biden directed DOJ to issue regulations prohibiting or restricting transactions involving bulk sensitive personal data and U.S. government-related data to countries of concern and covered persons. DOJ did so through an Advance Notice of Proposed Rulemaking ("ANPRM") published on March 4, 2024, and a Notice of Proposed Rulemaking ("NPRM") on October 29, 2024, before publishing a final rule on December 7, 2024.

## FINAL RULE OVERVIEW

DOJ's final rule establishes a new national security program within DOJ's National Security Division and anticipates parallel security requirements for restricted transactions that will be issued by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Agency ("CISA"). The rule restricts and, in some instances, prohibits, certain kinds of data transactions and access with six countries of concern and their covered persons, given the national security risks of those countries accessing Americans' bulk sensitive personal data.

## PROHIBITED, RESTRICTED, AND EXEMPT TRANSACTIONS

**Prohibited and Restricted Transactions.** The final rule prohibits and restricts data access and transactions with countries of concern and covered persons that involve sensitive personal data exceeding set bulk volume thresholds (discussed below). The rule prohibits data brokerage and covered data transactions involving access to bulk human 'omic data or human biospecimens from which 'omic data can be derived.[i] It restricts vendor, employment, and non-passive investment agreements. Notably, however, restricted transactions are permitted if they meet U.S. Department of Homeland Security's Cybersecurity and Infrastructure Agency ("CISA") security requirements, which relate to organizational cybersecurity, access controls, data security, and privacy. CISA published its final security requirements in January 2025.

## BULK THRESHOLDS TRIGGERING PROHIBITIONS AND RESTRICTIONS ON TRANSFER

The final rule defines "bulk" as any amount of sensitive personal data (even if anonymized, pseudonymized, de-identified, or encrypted) that exceeds certain thresholds, aggregated over the 12 months before a covered data transaction. The bulk thresholds are:

- human genomic data on over 100 U.S. persons, and the three other covered categories of human 'omic data on over 1,000 U.S. persons;
- biometric identifiers on over 1,000 U.S. persons;
- precise geolocation data on over 1,000 U.S. devices;
- personal health data and personal financial data on over 10,000 U.S. persons;
- certain covered personal identifiers on over 100,000 U.S. persons; or
- any combination of these data types that meets the lowest threshold for any category in the dataset.

The bulk thresholds do *not* apply to transactions involving U.S. government-related data, which are regulated regardless of volume.[ii]

**Exempt Transactions.** The final rule also exempts certain data transactions, including: personal communications; official U.S. government activities; certain financial services transactions; certain corporate group transactions; transactions required or authorized by federal law or international agreements; certain investment agreements; transactions ordinarily incident to telecommunications services; data transactions with countries of concern or covered persons involving drug, biological product, device, or combination product approvals or authorizations under certain conditions; and other clinical investigations and post-marketing surveillance data, again subject to certain conditions.

**Resale Risks**. The final rule notes that, to address resale risks, DOJ plans to issue compliance guidance that will include model contractual language requiring foreign persons to refrain from reselling or otherwise allowing countries of concern or covered persons to access sensitive data.

## COUNTRIES OF CONCERN AND COVERED PERSONS

The final rule designates six countries of concern: China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela. It also designates four classes of covered persons:

(1) foreign entities that are 50 percent or more owned by a country of concern, organized under the laws of 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 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.

These four categories are supplemented by a public list of DOJ-designated covered persons.

## LICENSING AND ADVISORY OPINION PROCESSES

**General and Specific Licenses.** The final rule authorizes DOJ to issue general licenses that authorize otherwise prohibited or restricted transactions and specific licenses for specific transactions. It also sets out the process for applying for a license or seeking reconsideration of a denied license.

**Advisory Opinions.** The final rule also permits regulated parties to ask DOJ to issue advisory opinions interpreting the regulations and addressing whether they are applicable to actual, specific transactions (not hypothetical transactions). In the final rule, DOJ notes that, in addition to publishing advisory opinions, it intends to publish general interpretive guidance—such as Frequently Asked Questions—online.

## RECORDKEEPING, AUDITING, REPORTING, AND COMPLIANCE REQUIREMENTS

A senior DOJ national security official has previously noted that the final rule requires covered U.S. companies and individuals to develop and implement "risk-based compliance programs tailored to their individualized risk profiles," similar to expectations in the sanctions and export control regime. DOJ notes that if a violation occurs, it will assess the adequacy of that compliance program in any enforcement action.

The final rule also clarifies that U.S. persons and companies engaging in restricted transactions must satisfy certain specific compliance obligations, including establishing a comprehensive compliance program. That program must include implementing risk-based procedures to:

- Verify and log data flows of sensitive personal and government-related data types and volume, transaction parties' identities, data end-use and transfer methods, and vendor identities;
- Establish written data security and compliance policies for restricted transactions that are certified annually by a responsible officer or employee;

- Conduct annual independent audits to verify compliance with CISA security requirements; and
- Maintain (and certify accuracy of) records for 10 years documenting data transfer methods, dates, agreements, licenses, and any other relevant documentation.

As noted above, CISA's finalized security requirements include technical elements and reflect practices that covered companies may not yet have in place.

**Reporting Requirements**. The final rule also establishes four specific reporting requirements:

*Cloud Computing.* Annual reports filed by U.S. persons engaged in restricted transactions involving cloud-computing services, if they are 25 percent or more owned, directly or indirectly, by a country of concern or covered person;

*Prohibited Transaction Offers.* Reports by any U.S. person that has received and affirmatively rejected an offer from another person to engage in a prohibited transaction involving data brokerage;

*Resale Restriction Violations (Known or Suspected).* Reports by U.S. persons engaged in a covered data transaction involving data brokerage with a foreign non-covered person if the U.S. 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

*Exemptions related to marketing drugs, products, or devices.* Reports by U.S. 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.

Companies can use existing audits and either internal or external audits (as long as they are independent) to satisfy these requirements.

## ENFORCEMENT MECHANISMS AND CIVIL AND CRIMINAL PENALTIES

As DOJ previewed, the final rule contains an enforcement strategy with "real teeth," backed by civil and criminal authorities under the International Emergency Economic Powers Act. It permits DOJ to conduct investigations, hold hearings, examine and depose witnesses, and issue subpoenas for witnesses and documents related to investigations of potential violations of the rule. It also permits civil and criminal penalties for violations. Civil penalties can be the greater of $368,136 or twice the amount of the transaction involved, while criminal penalties can include fines of up to $1,000,000 and up to 20 years' imprisonment.

Notably, DOJ advises that U.S. persons that provide third-party platforms or infrastructure are not civilly or criminally liable for customers' prohibited or restricted transactions on those platforms.

## WHAT TO EXPECT

The final rule goes into effect 90 days after it is published in the Federal Register, which is generally within a month of a rule's announcement. The rule's reporting requirements will become effective 270 days after that same publication. This means companies should expect that this rule—and its compliance and reporting requirements—will be fully in effect by late 2025.

Even though this EO was issued by President Biden, companies should not expect the coming change in administrations to slow enforcement of this rule. The national security risks posed by bulk data collection have received bipartisan attention, and addressing these risks enjoys broad support. We expect that the incoming presidential administration will be eager to enforce this rule, particularly given the Trump administration's persistent focus on the national-security threats posed by China.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,300 lawyers in 24 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered "Attorney Advertising."

View our Privacy Notice.

[i] EO 14117 lists several examples of "human 'omic data," including "human proteomic data, human epigenomic data, and human metabolomic data." EO 14117, § 6.

[ii] The final rule defines government-related data as:
(1) any precise geolocation data, regardless of volume, for any location within an enumerated government-related location data list that the Attorney General has determined poses a heightened risk of being exploited by a country of concern to reveal insights – such as about facilities, activities, or populations – about U.S.-government controlled locations, to the detriment of national security; (2) and any sensitive personal data, regardless of volume, that a transacting party markets as linked or linkable to current or former U.S. Government employees or contractors or former senior officials, including in the military or intelligence community.

# Special Matters & Government Investigations Partners

Gary Adamson
*New York*
+1 212 556 2113
gadamson@kslaw.com

Adam Baker
*New York*
+1 212 556 2376
abaker@kslaw.com

J.C. Boggs
*Washington, DC*
+1 202 626 2383
jboggs@kslaw.com

Christopher C. Burris
*Atlanta*
+1 404 572 4708
cburris@kslaw.com

Craig Carpenito
*New York*
+1 212 556 2142
ccarpenito@kslaw.com

Steve Cave
*Northern Virginia*
+1 703 245 1017
scave@kslaw.com

Michael J. Ciatti
*Washington, DC*
+1 202 661 7828
mciatti@kslaw.com

Daniel R. Coats
*Washington, DC*
+1 202 626 2642
dcoats@kslaw.com

Patrick M. Collins
*Chicago*
+1 312 764 6901
pcollins@kslaw.com

Ander M. Crenshaw
*Washington, DC*
+1 202 626 8996
acrenshaw@kslaw.com

Sumon Dantiki
*Washington, DC*
+1 202 626 5591
sdantiki@kslaw.com

Dan Donovan
*Washington, DC*
+1 202 626 7815
ddonovan@kslaw.com

Robert L. Ehrlich, Jr.
*Washington, DC*
+1 202 626 9710
rehrlich@kslaw.com

David Farber
*Washington, DC*
+1 202 626 2941
dfarber@kslaw.com

Zachary Fardon
*Chicago*
+1 312 764 6960
zfardon@kslaw.com

Emily Gordy
*Washington, DC*
+1 202 626 8974
egordy@kslaw.com

Leah B. Grossi
*Washington, DC*
+1 202 626 5511
lgrossi@kslaw.com

Ehren Halse
*San Francisco*
+1 415 318 1216
ehalse@kslaw.com

Ted Hester
*Washington, DC*
+1 202 626 2901
thester@kslaw.com

Max Hill, K.C.
*London*
+44 20 7551 2130
mhill@kslaw.com

Amy Schuller Hitchcock
*Sacramento/San Francisco*
+1 916 321 4819
ahitchcock@kslaw.com

John A. Horn
*Atlanta*
+1 404 572 2816
jhorn@kslaw.com

Andrew C. Hruska
*New York*
+1 212 556 2278
ahruska@kslaw.com

Rob Hur
*Washington, DC*
+1 202 383 8969
rhur@kslaw.com

Mark A. Jensen
*Washington, DC*
+1 202 626 5526
mjensen@kslaw.com

Dixie L. Johnson
*Washington, DC*
+1 202 626 8984
djohnson@kslaw.com

William Johnson
*New York*
+1 212 556 2125
wjohnson@kslaw.com

Barry Kamar
*Miami*
+1 305 462 6044
bkamar@kslaw.com

Allison F. Kassir
*Washington, DC*
+1 202 626 5600
akassir@kslaw.com

M. Alexander (Alec) Koch
*Washington, DC*
+1 202 626 8982
akoch@kslaw.com

Yelena Kotlarsky
*New York*
+1 212 556 2207
ykotlarsky@kslaw.com

Steve Kupka
*Washington, DC*
+1 202 626 5518
skupka@kslaw.com

Jade R. Lambert
*Chicago*
+1 312 764 6902
jlambert@kslaw.com

Jamie Allyson Lang
*Los Angeles*
+1 213 443 4325
jlang@kslaw.com

Raphael Larson
*Washington, DC*
+1 202 626 5440
rlarson@kslaw.com

Carmen Lawrence
*New York*
+1 212 556 2193
clawrence@kslaw.com

Brandt Leibe
*Houston*
+1 713 751 3235
bleibe@kslaw.com

Aaron W. Lipson
*Atlanta*
+1 404 572 2447
alipson@kslaw.com

Daniel E. Lungren
*Washington, DC*
+1 202 626 9120
dlungren@kslaw.com

William S. McClintock
*Washington, DC*
+1 202 626 2922
wmcclintock@kslaw.com

Amelia Medina
*Atlanta*
+1 404 572 2747
amedina@kslaw.com

Kendrick B. Meek
*Washington, DC*
+212 626 5613
kmeek@kslaw.com

Andrew Michaelson
*New York*
+212 790 5358
amichaelson@kslaw.com

Jim C. Miller III
*Washington, DC*
+1 202 626 5580
jmiller@kslaw.com

Patrick Montgomery
*Washington, DC*
+1 202 626 5444
pmontgomery@kslaw.com

Paul B. Murphy
*Atlanta/Washington, DC*
+1 404 572 4730
pbmurphy@kslaw.com

Grant W. Nichols
*Austin/Washington, DC*
+1 512 457 2006
gnichols@kslaw.com

Alicia O'Brien
*Washington, DC*
+1 202 626 5548
aobrien@kslaw.com

Patrick Otlewski
*Chicago*
+1 312 764 6908
potlewski@kslaw.com

Michael R. Pauzé
*Washington, DC*
+1 202 626 3732
mpauze@kslaw.com

Michael A. Plotnick
*Washington, DC*
+1 202 626 3736
mplotnick@kslaw.com

Olivia Radin
*New York*
+1 212 556 2138
oradin@kslaw.com

John C. Richter
*Washington, DC*
+1 202 626 5617
jrichter@kslaw.com

Rod J. Rosenstein
*Washington, DC*
+1 202 626 9220
rrosenstein@kslaw.com

Daniel C. Sale
*Washington, DC*
+1 202 626 2900
dsale@kslaw.com

Greg Scott
*Sacramento/San Francisco*
+1 916 321 4818
mscott@kslaw.com

Richard Sharpe
*Singapore*
+65 6303 6079
rsharpe@kslaw.com

Kyle Sheahen
*New York*
+1 212 556 2234
ksheahen@kslaw.com

Michael Shepard
*San Francisco*
+1 415 318 1221
mshepard@kslaw.com

Thomas Spulak
*Miami*
+1 305 462 6023
tspulak@kslaw.com

Aaron Stephens
*London*
+44 20 7551 2179
astephens@kslaw.com

Cliff Stricklin
*Denver*
+1 720 535 2327
cstricklin@kslaw.com

Jean Tamalet
*Paris*
+33 1 7300 3987
jtamalet@kslaw.com

Courtney D. Trombly
*Washington, DC*
+1 202 626 2935
ctrombly@kslaw.com

Rick Vacura
*Northern Virginia*
+1 703 245 1018
rvacura@kslaw.com

Anthony A. Williams
*Washington, DC*
+1 202 626 3730
awilliams@kslaw.com

David K. Willingham
*Los Angeles*
+1 213 218 4005
dwillingham@kslaw.com

David Wulfert
*Washington, DC*
+1 202 626 5570
dwulfert@kslaw.com

Sally Q. Yates
*Atlanta/Washington, DC*
+1 404 572 2723
syates@kslaw.com