Articles + Publications | April 3, 2025

New DOJ National Security Division Data Security Rules Take Effect on April 8: Is Your Organization Exposed?

WRITTEN BY

James Koenig | Laura Hamady | Peter E. Jeydel | David J. Navetta

What's Happening?

Under the Department of Justice's (DOJ) "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons" rules (the Rules), allowing access outside the United States to certain types of sensitive personal data involving "countries of concern" may be restricted or prohibited beginning on April 8. See our previous advisory for more detail.

Who May Be Impacted?

These Rules will apply to a wide variety of organizations that engage in "covered data transactions" involving China, Russia, Iran, Cuba, Venezuela, or North Korea, or "covered persons" linked to those countries.

The Rules also apply to "data brokerage" activities involving covered data with no link to any of those countries or persons. Data brokerage is defined very broadly as "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."

What Is Covered Data?

1. In a 12-month period, data collected about or maintained on:

a. Human genomic data: more than 100 U.S. persons;

b. Other human `omic data: more than 1,000 U.S. persons;

c. Biometric identifiers: more than 1,000 U.S. persons;

d. Precise geolocation data: more than 1,000 U.S. devices;

e. Personal health data: more than 10,000 U.S. persons;

f. Personal financial data: more than 10,000 U.S. persons;

g. Covered personal identifiers: more than 100,000 U.S. persons; or

h. Combinations of the above meeting the lowest applicable threshold.

2. Government-related data, regardless of volume, including either:

a. Precise geolocation data for any location within any area enumerated on the Government-Related Location Data List in § 202.1401; or

b. Covered personal identifiers, precise geolocation data, biometric identifiers, human `omic data, personal health data, personal financial data, or any combination thereof, marketed as linked or linkable to current or recent former employees or contractors, or former senior officials, of the U.S. government.

Are My Existing Compliance Programs Enough?

Having a robust data governance program will help, but there are material differences between these new DOJ Rules and existing data protection laws. Similarly, these Rules do not look or act like existing export controls or sanctions regimes. These DOJ regulations are premised on national security concerns and will require a unique and additive compliance approach.

Can It Wait?

No. The Rules take effect on April 8. The Trump administration is focused on national security concerns with China and other "adversaries" covered by these Rules. We expect aggressive enforcement to begin this year.

What Happens If We Don't Comply?

These are national security rules with strict civil and criminal penalties, based on the same statutory penalty structure that applies under U.S. economic sanctions. This can include large fines (civil penalties of up to $368,136 per violation or twice the amount of the transaction involved; and criminal fines up to $1 million per violation) and imprisonment up to 20 years. The National Security Division prosecutors enforcing these Rules will likely take an aggressive approach to penalties based on their mandate. Because these penalty amounts apply *per violation*, they can be multiplied into very large penalties.

What Can We Do?

Assessing whether and how the Rules apply to your organization is the first step. Our cross-functional national security and cyber/privacy groups can assist your company in understanding its obligations by helping you get started with a scope review for a fixed fee. This includes a set of questionnaires and an initial consultation about the Rules and how to conduct this analysis. We are also available to guide your organization through the full scope review, as well as additional compliance, documentation, or implementation/remediation steps, based on the outcome of your scope review.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber