WILLKIE

CLIENT ALERT

The Federal Data Protection Regime You May Not Know Is Coming: DOJ's Bulk Data Transfer Rules

April 1, 2025

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Susan E. Rohol

A new federal data protection regime that many people may not know about – but which will have significant implications for companies across the country – is coming into effect next week. Specifically, the Department of Justice ("DOJ"), in conjunction with the Cybersecurity and Infrastructure Security Agency ("CISA"), adopted the so-called "Bulk Data Transfer Rules" in response to a February 2024 Executive Order from President Biden. These rules are intended to protect Americans' sensitive personal data, as well as U.S. government data, from being transferred to "countries of concern," which include China, Cuba, Iran, North Korea, Russia and Venezuela. The rules prohibit or restrict U.S. persons from knowingly engaging in "covered data transactions" with the listed countries of concern or "covered persons" (defined below). There are two key compliance dates:

- By April 8, 2025, companies that engage in such transactions must either stop all prohibited transactions or employ the protections established by CISA for "restricted" transactions.

- By October 6, 2025, companies that engage in restricted transactions must have implemented a broad "know-your-data" program that imposes significant recordkeeping and diligence requirements.

While the rules may target the transfer of certain data to entities or countries that could harm U.S. national and economic security interests, their requirements are actually quite broad, and potential penalties for non-compliance – including both criminal and civil penalties – are significant. At the very least, many companies will want to consider policies, new safeguards, and additional diligence of partners, service providers, and even employees, even if only to ensure that they are not engaging in prohibited or restricted transfers.

Types of Covered Data

The rules cover two types of data: bulk sensitive personal data of U.S. persons and Government-related data.

The rules establish six categories of "sensitive personal data":

- covered personal identifiers (defined to include, among other things, a number of different categories of identifiers, such as demographic information, contact information, and device identifiers, when combined with other covered personal identifiers);
- precise geolocation data (defined more broadly than most state privacy law definitions);
- biometric identifiers;
- human 'omic data;
- personal health data; and
- personal financial data.

Bulk thresholds are defined for each category. For example, precise geolocation data collected about or maintained on more than 1,000 U.S. devices qualifies as "bulk."

Government-related data is defined as "[a]ny precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List," and "[a]ny 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." DOJ explained that the "marketed as" qualifier should allow companies to avoid a situation where they have to, for example, "ask individuals whether they are former government employees when collecting their data."

One aspect of these definitions that has generated significant concern is that deidentified data is *not* per se excluded, as it is for terms like "personal information" and "personal data" in many state and federal privacy laws. DOJ's decision to refrain from excluding deidentified data focused on the ability of adversaries to reidentify data through the compilation of significant and broad data sets. This does not necessarily add to the amount of data that may be at issue – data still must qualify as sensitive personal data under the definitions summarized above – but it does potentially complicate compliance efforts for companies that would like to leverage existing privacy and data protection efforts.

Covered Data Transactions

"Covered data transactions" are transactions involving bulk U.S. sensitive personal data or government-related data. Transactions are categorized as prohibited or restricted, with specific definitions for data brokerage, vendor agreements, employment agreements, and investment agreements. Data brokerage transactions are prohibited entirely, while vendor, employment, and investment agreements are restricted unless robust security requirements are implemented.

- A "data brokerage" transaction is "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." This definition is arguably broader even than some current state laws, which focus on the relationship of the provider to the consumer.

- A "vendor agreement" is "any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration."

- An "employment agreement" is "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."

- An "investment agreement" is "an 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: (1) Real estate located in the United States; or (2) A U.S. legal entity." The definition expressly carves out "passive" investments, defined to include investments in publicly traded securities.

In parallel with the DOJ rulemaking, the Cybersecurity and Infrastructure Security Agency (CISA) adopted security requirements for entities engaging in restricted transactions. These requirements include organizational and service-level requirements, as well as data-level requirements. CISA sought to align the requirements with both the

NIST Cybersecurity Framework and NIST Privacy Framework, to provide some flexibility and additional direction to entities as they implement specific safeguards.

Finally, there are classes of transactions that may qualify as "covered data transactions," but which are exempt. Categories of exempt transactions include personal communications, financial services, telecommunications services, and corporate group transactions, and are narrowly defined. For example, the corporate group transactions exemption "may apply to situations in which employees of a U.S. company's affiliate located in a country of concern are provided with access to covered data," but the exemption is highly specific to the nature of the activity for which the data is being transferred. Moreover, exempt transactions will still require substantial compliance efforts, even just to analyze and document whether an exemption applies.

Countries of Concern and Covered Persons

As noted, countries of concern include China, Russia, Iran, North Korea, Cuba, and Venezuela. Covered persons are defined based on ownership, control, and residency criteria. For example, an entity would be a covered person if it is "[a] foreign person that is an entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by one or more countries of concern or covered persons or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern."

"Know-Your-Data" and Diligence Requirements

The "knowingly" standard adopted in the rules is arguably better described as a "knew or should have known" standard, and this will likely force many companies to adapt their compliance efforts to these new rules, even if they do not today engage in any prohibited or restricted transactions. In particular, the rules include a "know-your-data" requirement designed to ensure companies know – or should have known – whether they are engaging in these transactions. Under this requirement, by October 6, 2025 companies that engage in any restricted transactions must have in place a compliance program comprised of the following components:

- Risk-based procedures for verifying data flows involved in any restricted transaction, including procedures to verify and log, in an auditable manner: (i) the types and volumes of covered data involved in the transaction; (ii) the identity of the transaction parties, including any ownership of entities or citizenship or primary residence of individuals; and (iii) the end-use of the data and the method of data transfer;
- For restricted transactions that involve vendors, risk-based procedures for verifying the identity of vendors;
- A written policy that describes the data compliance program and that is annually certified by an officer, executive, or other employee responsible for compliance; and
- A written policy that describes the implementation of the CISA security requirements and that is annually certified by an officer, executive, or other employee responsible for compliance.

Moreover, as part of the compliance program, companies must keep "full and accurate records" of restricted transactions for at least 10 years. The rules include detailed requirements for what those records should include, such as documentation of the due diligence conducted to verify the data flow involved in any restricted transaction and an annual certification by an officer, executive, or other employee responsible for compliance of the completeness and accuracy of the records documenting due diligence.

Next Steps

The immediate concern for any companies that may be subject to these rules is to identify potentially in-scope data and transactions and consider whether those transactions must be stopped in light of the looming April 8, 2025 effective date. More broadly, though, even companies that do not today engage in any covered data transactions will likely want to consider employing steps to avoid such transactions in the future. For example, the diligence requirements only apply to companies engaged in restricted transactions, but companies that find themselves subject to a DOJ investigation will likely want to have policies, records, and similar documentation in place to demonstrate to DOJ that they are *not* engaged in such transactions.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez	Laura E. Jehl	Susan E. Rohol
202 303 1125	202 303 1056	310 855 3172
dalvarez@willkie.com	ljehl@willkie.com	srohol@willkie.com

WILLKIE

BRUSSELS CHICAGO DALLAS FRANKFURT HOUSTON LONDON LOS ANGELES MILAN
MUNICH NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON