October 03, 2025

Kelly DeMarchis Bastide, Jennifer Daskal, Rob Hartwell and Matthew Stern

October 6 New Compliance Deadlines: DOJ's Bulk Data Rule

4min

The Department of Justice's (DOJ) Final Rule, Preventing Access to U.S. Sensitive Personal Data and Government Related Data by Countries of Concern or Covered Persons (the "Bulk Data Rule"), effective since April 8, 2025, is entering a critical new phase. While the applicable prohibitions and restrictions on covered transactions came into effect several months ago, companies were given an additional six months to put in place required data compliance programs and carry out additional compliance obligations.

That effective date—*October* 6, 2025—is fast approaching.

Background

As described in multiple prior alerts, the Bulk Data Rule *prohibits* the direct sale or transfer of bulk sensitive data about U.S. persons and certain U.S. government-related data to "countries of concern"—currently, China, Cuba, Iran, North Korea, Russia, and

Venezuela—and "covered persons." The sale or transfer of such data to all other foreign countries and persons is also prohibited, unless accompanied with contractual provisions to prevent onward transfer of such data to a country of concern or covered person.

The rule *restricts* other transactions—namely those that include vendor, employment, or investment agreements that involve access to bulk U.S. sensitive data or government data by a country of concern or covered person. Restricted transactions are permitted if they comply with the security requirements promulgated by the Cybersecurity and Infrastructure Security Agency (CISA), along with the other applicable due diligence, auditing, and reporting obligations that go into effect on October 6.

The key purpose of the rule is to stop foreign adversaries from accessing U.S. government-related data and Americans' sensitive personal data. The concern: Foreign adversaries can use such data to conduct surveillance and economic espionage, develop AI and military capabilities, and otherwise undermine the United States' national security.

What's Already in Effect?

Companies are already required to comply with the prohibitions and restrictions laid out above. In order to do so, companies should map their data to understand whether and to whom they are transferring covered data, update transfer agreements to include necessary restrictions on onward transfers, evaluate vendors and employment contracts, and, if needed, implement cybersecurity measures that meet CISA standards. (If your company is potentially

covered by the rule and has not yet done these things, we can help!)

What's Coming into Effect?

Effective October 6, 2025, U.S. persons engaged in covered transactions must comply with the following additional requirements, among others:

1. **Maintain a data compliance program** that includes risk-based procedures for verifying and logging covered data flows, the identity of relevant vendors, and implementation of applicable security requirements. 8 C.F.R. § 202.1001
2. **Perform annual audits** to verify compliance with security and data handling requirements. § 202.1002
3. **Report offers** to engage in prohibited transactions. § 202.1104
4. **Submit an annual report** if engaging in a restricted transaction involving cloud-computing services and the entity involved is 25% or more owned directly or indirectly by a country of concern or a covered person. Id. § 202.1103
5. **Maintain records** of data compliance program; implementation of applicable security requirements; audits; covered transactions; and other specified documents. § 202.1101

Why Does It Matter?

Failure to comply could lead to criminal liability and significant civil penalties. Although there have been no enforcement actions to date, the Rule is relatively new, and in previously released guidance,

DOJ has signaled a continued focus on ensuring compliance with the rules.

Meanwhile, some companies have already faced civil lawsuits for allegedly violating both the Electronic Communications Privacy Act and the Bulk Data Rule.

Broad Applicability

This rule applies broadly—covering just about any company that handles bulk U.S. sensitive personal data or government-related data and engages internationally. This includes any company that handles biometric identifiers (like fingerprints or facial scans); human genomic, geolocation data, personal financial, and health information; and personal identifiers such as names, addresses, Social Security numbers, and IP addresses, when such personal identifiers are used in combination with one another.

Venable's Privacy and Data Security Practice Group and Cybersecurity Services Practice Group have extensive experience counseling clients on Bulk Data Rule compliance. Please reach out for support in understanding how the Bulk Data Rule applies to your business and how to effectively comply.

Related Services

Practices

Privacy and Data Security

Industries

Cybersecurity Services

Related Insights

"Baby FARA" Laws Are Growing Up: State-Level Disclosure of Foreign Relationships Is Here

8min

September 25, 2025

Executive Order to Prevent Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern

11min

March 04, 2024

Key Insights: DOJ's Proposed Rule to Protect Bulk Sensitive Personal Data—What Companies Need to Know

10min

November 04, 2024

Recent News

Venable Serves as Outside Counsel for Harlem's Studio Museum Grand Reopening

3min

October 06, 2025

Venable Adds Private Wealth Planning Veteran David Berek as Partner in Chicago

3min

October 01, 2025

The Celebrity Estates: Wills of the Rich and Famous Podcast Interviews Kevin

1min

Ghassomian on Armani's Estate Planning Strategies

September 29, 2025