March 17, 2025

Kelly DeMarchis Bastide, Michael A. Signorelli, Rob Hartwell and Matthew Stern

A Brave New World: Four Considerations When Building a Bulk Data Rule Compliance Program

8min

U.S. companies and organizations have entered a new era of sweeping restrictions on cross-border data transfers. 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"), will take effect on April 8, 2025, with certain requirements coming into effect on October 6, 2025.[1] For an overview of the Bulk Data Rule, please read our prior summaries. When considered with the Protecting Americans' Data from Foreign Adversaries Act (PADFAA), which went into effect on June 23, 2024, the U.S. now has a robust set of restrictions imposed on transfers of specific data types from the U.S. to certain countries designated as "countries of concern" or "foreign adversaries," a list that includes China and Russia.[2] Accordingly, any organization that engages in data transfers or provides access to covered data about U.S. individuals to China,

Russia, and other specified countries or companies or individuals "controlled by" those countries needs to navigate these new restrictions and evaluate their data practices for applicability under the relevant regime(s) and build a compliance program to meet the new demands of this framework. A reasonable compliance program can also be helpful in establishing that any unintentional violation of the Bulk Data Rule was done without the requisite "knowledge" required for a violation to occur.

This alert focuses on the Bulk Data Rule and provides some initial considerations when developing a go-forward strategy to identify and address implicated data transactions. Companies and organizations should determine if their practices are impacted by these restrictions, and, if so, they should develop a compliance program to manage the ongoing diligence, auditing, reporting, security, and recordkeeping required for these transactions. While the contours of any compliance program will be unique, we highlight below four stepping-stones for building a cross-border data compliance program.

1. Identifying Covered Data and Data Transactions Is a Crucial First Step.

The broad scope of the Bulk Data Rule presents a significant challenge. Unlike PADFAA, which limits its scope to "data brokers" and their related activities, the Bulk Data Rule prohibits and/or restricts many types of ordinary business transactions for any U.S. entity, including routine customer, vendor, employee, and investor transactions that involve the flow of data to entities or individuals

in a country of concern.[3] For a large organization, thousands of contractual agreements may be implicated and will need to be assessed for termination or further action. The Bulk Data Rule also differs from PADFAA by addressing "data brokerage" to foreign persons that are not prohibited from receiving data by imposing a requirement to include contractual obligations limiting "onward transfer" from those foreign persons to covered persons.[4]

Although the Bulk Data Rule's "covered data" is limited by volume thresholds, they are, in some cases, quite modest. For example, "bulk" amounts of sensitive personal data are defined as meeting or exceeding the following thresholds: 1) human genomic data on over 100 U.S. persons; 2) biometric identifiers on over 1,000 U.S. persons; 3) precise geolocation data on over 1,000 U.S. devices; 4) personal health data on over 10,000 U.S. persons; 5) personal financial data on over 10,000 U.S. persons; and 6) certain covered personal identifiers (including IP addresses, device IDs, and names and email addresses) for more than 100,000 U.S. persons. These thresholds are calculated by determining whether, in the preceding 12 months, through a single covered data transaction or aggregated across covered data transactions involving the same U.S. person and same foreign person or covered person, the thresholds were satisfied.[5]

As an initial step, organizations should leverage existing internal processes to identify higher-risk data systems and processing or sharing arrangements for priority assessment. This could include contract or vendor management databases or processes, any existing data maps of inventories, or records of processing. These include not only such data-sharing arrangements when they are externally facing, but also potentially internal data transfers

between affiliates or subsidiaries and even human resources functions that may provide access to vendors or employees who are covered persons. These resources can help determine which transactions that are already under way may include implicated data types or recipients. These documents, however, may not address all relevant considerations for the Bulk Data Rule and may need to be augmented with additional internal review. Moreover, the Bulk Data Rule contains numerous exemptions and exceptions that can render "out of scope" many types of transactions. Understanding the purpose(s) of any data transfers and documenting this evaluation will be crucial to preserving (and rendering compliant) existing data flows.

Enlisting the support of various functions—IT, marketing, HR—will be helpful, as they know their area of responsibility best. In some cases, you may need to gather additional information about the recipient, employee, or vendor, including whether their ownership structure or primary residence implicates the rule. For example, data recipients with 50% or more ownership by people or entities in countries of concern are covered, even if those owners do not interact with your organization's covered data. Development of questionnaires, review of corporate information databases, and leveraging other standardized materials can help streamline the information-gathering and assessment process.

2. Some Transaction Types May Be Prohibited and Stopped by April 8.

With the short timeline to prepare for the Bulk Data Rule, organizations must quickly come to terms with the reality that

some transactions may simply be prohibited and must be terminated or restructured in short order. For example, the Bulk Data Rule classifies as "sensitive" certain types of personal data that businesses may already process with heightened safeguards: health, biometric, genetic, financial, and precise geolocation data. Such data is often subject to unique data security requirements or data-processing restrictions under U.S. federal or state privacy laws. To meet these existing obligations, businesses often employ various tools and additional measures, like de-identification and anonymization, to be able leverage this data in a way that does not infringe existing laws.

Under the Bulk Data Rule, such tools and techniques cannot be employed to remove data from the Bulk Data Rule's requirements. For example, the Bulk Data rule would classify as "prohibited" the transfer of health data of 10,000 persons, *even if* such data is anonymized or de-identified.[6] The definition of health data is broad enough to include data elements such as height and weight that are routinely collected and considered benign in many circumstances. If transfers of such data are integral to your services, you will need to find an alternative. Involving business stakeholders in these discussions sooner rather than later can help ensure sufficient time is allotted to cease the data flows and set up workarounds.

3. You Will Need to Build a Compliance Program.

Besides prohibited transactions, the Bulk Data Rule also creates a classification of transactions designated as "restricted." Restricted

transactions involve covered data processed pursuant to a vendor agreement, employment agreement, or investment agreement, and may proceed only when the U.S. person complies with certain security and audit requirements. These detailed security requirements must be implemented to continue the flow of data subject to these third-party arrangements by the April 8 compliance data.

The Bulk Data Rule requires businesses to create a data compliance program no later than October 6, 2025 that includes formal policies and risk-based evaluation tools for all such third-party arrangements. In addition, such transactions are required to go through an independent, annual audit process and are subject to certain data security requirements. The documentation surrounding restricted transactions is also subject to formal recordkeeping requirements. Thus, businesses engaged in restricted transactions will need to build and document a new third-party risk process and begin the process of running all implicated third-party arrangements through formal risk assessment before the end of the year.

Organizations should look to any existing vendor management and audit programs as an initial starting point when building this program internally, with the awareness that these processes will not be wholly sufficient on their own. The Bulk Data Rule imposes specific requirements unique to it, for managing restricted transfers going forward. Moreover, restricted transfers not only have to be identified and addressed, but formally documented, and the entire program is subject to an annual certification by a responsible employee, officer, or executive. The governance

requirements may be significant in terms of time and resources.

4. More Guidance May Be Forthcoming.

The Biden DOJ indicated that further public guidance on compliance would be issued before the Bulk Data Rule becomes effective next month.[7] No such guidance has been issued to date.

For instance, the DOJ stated that it anticipates providing sample contractual language to satisfy the requirement discussed above related to restricting foreign persons (non-covered) from conducting onward transfers to covered persons or countries of concern.[8] The DOJ also expressed its intent to publish other general guidance, such as Frequently Asked Questions.[9]

The Bulk Data Rule also permits any U.S. person engaged in transactions that may be regulated by the regime to request an advisory opinion from DOJ about the interpretation and application of the rule to actual specific transactions, not hypothetical, anonymous situations.[10] This formal opportunity to request an advisory opinion may serve as a built-in compliance check for businesses to determine whether certain transactions are within the scope of the rule.

About Venable

Venable's Privacy and Data Security Practice Group has extensive experience counseling clients on their obligations under federal and state privacy laws. Please feel free to reach out to us if you

would like to learn more about how we can help with data transfers and what you can do to assess your compliance posture with respect to new laws or regulations.

---

[1] Available at Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons (hereinafter, "Bulk Data Rule").

[2] Pub. Law. No. 118-50 (I)(2)(c)(4) (defining foreign adversary countries as those listed in 10 U.S.C. § 4872(d)(2)); Bulk Data Rule § 202.601. The current list of countries of concern is China, Cuba, Iran, North Korea, Russia, and Venezuela, but others may be designated in the future.

[3] Bulk Data Rule §§ 202.301, 202.401.

[4] § 202.302.

[5] § 202.205.

[6] §§ 202.205, 202.241.

[7] DOJ Fact Sheet, available here.

[8] Bulk Data Rule's Discussion of Comments on the Notice of Proposed Rulemaking and Changes from the Proposed Rule, A. General Comments.

[9] *Id.* at H. Subpart I—Advisory Opinions.

[10] § 202.901.

Related Services

Practices

- Privacy and Data Security

Related Insights

Key Privacy Issues in Adtech

1min

April 03, 2025

Laws Regulating Minors' Access to Social Media Face First Amendment Scrutiny in the Courts

6min

March 11, 2025

Event in Review: Navigating the Privacy Landscape—Trends to Watch in 2025

3min

March 05, 2025

Events

Leave No Crumbs: Practical Tips for Cookie Compliance and Litigation Defense

---

May 07, 2025 - Washington, DC - Privacy + Security Academy

Recent News

Derek Smith Joins International Association of Defense Counsel

1min

April 23, 2025

Joshua Rosenberg and William Briggs Recognized Among *Billboard*'s Top Music Lawyers for 2025

1min

April 22, 2025

Michael Garfinkel Named Among *Los Angeles Business Journal*'s 2025 Top 100 Lawyers in Los Angeles

1min

April 22, 2025
