CLIENT ALERTS & INSIGHTS

Businesses Must Be Ready for Additional October Compliance Obligations under the DOJ's Bulk Data Transfer Rule when Interacting with Countries of Concern and Covered Persons

AUGUST 22, 2025

Authors: Michael D. Stovsky, Trevor Martin, Kristopher J. Chandler

On April 8, 2025, the Bulk Data Transfer Rule went into effect. It became enforceable on July 8, 2025; however, many of the technical enforcement obligations under the Bulk Data Transfer Rule become enforceable on October 6, 2025 (the "Deadline"), which is the final compliance deadline in the DOJ's rollout of the Bulk Data Transfer Rule. The Bulk Data Transfer Rule has broad implications for data transactions and transfers. By the Deadline, U.S. businesses must implement due diligence requirements for full compliance with the Bulk Data Transfer Rule, including security, privacy, records, and reporting requirements.

Background

The Bulk Data Transfer Rule regulates transactions involving two types of data (together, "**Covered Data**"):

1. **U.S. sensitive personal data** - six sub-categories, each with 12-month "bulk" thresholds for transacting parties: covered personal identifiers (100,000 U.S. persons), precise geolocation data (1,000 U.S. devices), biometric identifiers (1,000 U.S. persons), human 'omic data[1] (100 U.S. persons for human DNA sequences or testing results; 1,000 U.S. persons for higher ("systems-") level data regarding gene expression), personal health data (10,000 U.S. persons), and personal financial data (10,000 U.S. persons); and
2. **U.S. government related data** - two sub-categories without "bulk" thresholds: precise geolocation data for any location within any area enumerated on the Government-Related Location Data List or any sensitive personal data that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the U.S. government, including the military and intelligence community.

The Bulk Data Transfer Rule regulates transactions of Covered Data between U.S. businesses and designated "countries of concern", or between U.S. businesses and "covered persons" (persons or entities located in countries of concern or which are owned by countries of concern or covered persons. There are currently six countries that are designated under the Bulk Data Transfer Rule as countries of concern: China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela, as well as entities and individuals under their control. Transactions involving the

transmission of Covered Data to countries of concern or covered persons are called “Covered Data Transactions.” Specifically, the Bulk Data Transfer Rule:

- prohibits Covered Data Transactions consisting of (A) 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; or (B) that involves access to bulk human ’omic data or to human biospecimens from which covered data could be derived (“Prohibited Transactions”); and

- restricts other Covered Data Transactions involving an employment agreement, vendor agreement, or investor agreement with a country of concern or a covered person (“Restricted Transactions”).

The Bulk Data Transfer Rule exempts certain categories of data transactions (“ Exempt Transactions ”):

- personal communications (postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value);
- information or informational materials (importation from any country or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials);
- travel (to the extent that they are ordinarily incidental to travel to or from any country, including importation of accompanied baggage for personal use, maintenance within any country, including payment of living expenses and acquisition of goods or services for personal use, or the arrangement or facilitation of such travel, including nonscheduled air, sea, or land voyages);
- transfers that are necessary for compliance with U.S. legal obligations;
- transfers that occur within a U.S.-based entity and do not involve foreign persons or entities;
- transfers that are not reasonably likely to result in access by a “covered person” or a “country of concern”; or
- official business of the U.S. government.

This means that intracompany transmissions-such as data shared between departments or subsidiaries of the same U.S. company-may be exempt if:

- The data does not leave the U.S. jurisdiction; or
- The transmission does not involve foreign affiliates in countries of concern.

Enforcement Penalties

Violations of the Bulk Data Transfer Rule carry with them penalties in the amount of the greater of (i) **$368,136 per violation**; or (ii) an amount twice the size of the transaction that is the basis of the violation. Willful violations may result in criminal penalties of fines **up to $1,000,000 or up to 20 years in prison**.

Compliance Steps

By the Deadline, U.S. businesses must have aligned their internal practices with the Bulk Data Transfer Rule, including, as applicable:

All U.S. Businesses:

1. internal reviews of access to Covered Data, including whether transactions involving access to such data flows constitute Prohibited Transactions; and
2. reviews of internal datasets and datatypes to determine if they are potentially subject to the Bulk Data Transfer Rule.

U.S. Businesses engaged in Covered Data Transactions:

1. cease conducting Prohibited Transactions and Restricted Transactions that fail to comply with the Bulk Data Transfer Rule's technical requirements;
2. (re)negotiate vendor agreements, including negotiating contractual onward transfer provisions with foreign persons who are the counterparties to Covered Data Transactions;
3. transfer products and services to new vendors, if unable to (re)negotiate terms for compliance with the Bulk Data Transfer Rule;
4. implement a process to conduct due diligence on potential new vendors;
5. adjust employee work locations, roles, or responsibilities;
6. evaluate investments from countries of concern or covered persons to determine whether they are potentially subject to the Bulk Data Transfer Rule;
7. perform due diligence on the ownership structure of vendors and other contractors, data processors, and service providers to which Covered Data is transferred, through multiple tiers of ownership, to determinate whether a vendor's ownership structure renders the transfer of Covered Data subject to the Bulk Data Transfer Rule; and
8. renegotiate investment agreements with countries of concern or covered persons for compliance with the Bulk Data Transfer Rule.

Businesses engaged in Restricted Transactions:

Implement the following internal programs:

1. Data Compliance: written, risk-based policies and procedures for verifying data flows involved in Restricted Transactions that meet the Cybersecurity and Infrastructure Agency ("CISA") Security Requirements for Restricted Transactions ("Security Requirement") and are annually certified by an officer, executive, or other employee responsible for compliance.
2. Audit: procedures for conducting annual, independent audit to examine, verify, and attest to compliance with and the effectiveness of the Bulk Data Transfer Rule's Security Requirement.
3. Records Keeping: policies and procedures for maintaining full and accurate records of each Restricted Transaction or Prohibited Transaction for 10 years after the transaction date and written policies regarding the same.
4. Reporting: policies and procedures for compiling and submitting (A) annual reports regarding Restricted Transactions and Prohibited Transactions involving cloud-computing services if the business's equity interests are owned (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise) by a country of concern or covered person; and (B) reporting of a business's rejection of an offer from another person to engage in a Restricted Transaction or Prohibited Transaction involving data brokerage.

Conclusion

As the Deadline approaches for the Bulk Data Transfer Rule's due diligence requirements, businesses must continue to take proactive steps to understand and implement the rule's complex compliance requirements. Navigating this regulatory shift demands not only technical precision but also strategic legal insight. From assessing data transfer practices to updating contractual frameworks and internal controls, the stakes are high for organizations that handle sensitive personal data or government related data. The history and policy behind the Bulk Transfer Rule point to proactive enforcement, and the risks and consequence of non-compliance will likely increase. Maintaining a proactive data compliance program that can effectively and timely respond to changes in the law, agency, and new risks is critical.

Benesch is closely monitoring developments and advising clients across industries on tailored compliance strategies. If your business may be impacted by the Bulk Data Transfer Rule, we invite you to contact **Benesch's Data Protection team** for assistance navigating readiness and risk in this evolving regulatory landscape.

[1] The Bulk Transfer Rule treats human 'omic data as the most sensitive type of U.S. personal data; however, what defines "human 'omic" is complex and untested. Accordingly, U.S. businesses that collect, hold, or otherwise processes datasets consisting or derived from human DNA sequences should be scrupulous in their transfer.