DOJ's Data Security Rule: New Limits on Cross-Border Data Transfers

By Tom Langan

Background

On April 8, 2024, the U.S. Department of Justice ("DOJ") issued the Data Security Rule (the "Rule"), under its Data Security Program ("DSP"). Authorized by Executive Order 14117, the Rule addresses national security risks from the "weaponization" of sensitive U.S. personal and government-related data. It restricts cross-border data transfers, including intracompany transactions, with "countries of concern" (China, including Hong Kong and Macau, Cuba, Iran, North Korea, Russia, and Venezuela). Because noncompliance can expose clients to significant penalties, Legalink members advising clients in IP, IT, and data protection must understand the Rule's requirements.

What Does the Rule Cover?

The Rule governs "covered data transactions" that provide "countries of concern" or "covered persons" (e.g., entities or individuals tied to these nations) access to:

- Bulk U.S. Sensitive Personal Data: Includes genomic data (1,000+ persons), biometric identifiers (1,000+ persons), precise geolocation data (1,000+ devices), personal health or financial data (10,000+ persons), or covered personal identifiers (100,000+ persons, e.g., Social Security numbers linked to other identifiers).
- Government-Related Data: Precise geolocation data near sensitive government sites or data linked to U.S. government personnel, regardless of volume.

The Rule applies to all "U.S. persons" (citizens, lawful residents, U.S.-organized entities, or anyone in the U.S.). However, it does not apply to transactions completed prior to April 8, 2025, but the DOJ may ask for records of these transactions.

What Transactions Are Prohibited or Restricted?

Covered transactions fall into two categories: (1) prohibited and (2) restricted:

- Prohibited Transactions: Without a DOJ license, U.S. persons cannot knowingly engage in data brokerage with countries of concern, transactions involving bulk human 'omic (e.g., genomic or biometric) data, or other transactions undertaken to evade the Rule. An exception allows data brokerage with non-covered foreign persons if contracts prohibit onward transfers to countries of concern and violations are reported within 14 days.

- Restricted Transactions: Under the Rule, vendor, employment, and investment agreements must comply with Cybersecurity and Infrastructure Security Agency (CISA) standards, including specific encryption and access controls. Due to the strict CISA requirements, transactions involving bulk genomic data are effectively prohibited.

What Are the Compliance Requirements?

U.S. persons must:

- Perform due diligence to identify data types and recipients to avoid prohibited transactions.
- Retain records of covered data transactions for at least 10 years.
- Conduct annual independent audits for restricted transactions and file reports for certain cloud-computing services if 25%+ equity is held by a country of concern.
- Request DOJ advisory opinions if it is unclear whether a transaction is compliant. The DOJ intends to provide a response within 30 days.

The DOJ has released a Compliance Guide and FAQ to assist organizations in understanding and complying with the Rule: https://www.justice.gov/nsd/data-security Beginning October 6, 2025, U.S. persons must also fulfill specific due diligence and audit requirements before engaging in restricted transactions, as outlined in the Compliance Guide and FAQ.

What Are the Penalties?

Violations are subject to civil fines in excess of $350,000 per violation (or twice the transaction value) and criminal penalties of up to $1 million or 20 years' imprisonment for willful acts. Penalties vary in severity, considering the violator's level of sophistication and whether the violator has attempted to evade the Rule.

Are There Exceptions?

Narrow exceptions to the Rule include transactions for personal communications that do not involve the transfer of anything of value, transactions that are ordinarily incident to international travel, U.S. government business, transactions incident to financial services (e.g., payment processing) and transactions incident to corporate administrative operations (e.g., payroll and human resources). Additionally, the DOJ has a licensing structure to allow some prohibited transactions, although it anticipates granting only limited numbers of licenses, and currently, no licenses are publicly available.

What's Next for Legalink Members?

The Rule poses complex challenges for clients, especially in technology, healthcare, and finance. Organizations (with the assistance of counsel) should assess their data holdings and identify sensitive data that might be subject to the Rule, including in connection with existing contracts and data-sharing agreements. Organizations should also work proactively to develop compliance programs that are tailored to conform to DOJ guidance. Counsel should also advise clients to proactively obtain advisory opinions from the DOJ if there is any doubt regarding whether complex transactions are compliant.

Given the Rule's complexity, organizations should act now to assess data practices and implement compliance measures. Because the DOJ will enforce the Rule much more strictly for knowing violators, clients can avoid the worst legal exposure through best efforts at good faith compliance. Contact us at Dvorak Law Group and visit https://www.justice.gov/nsd/data-security for more information.