



Insights

Compliance Obligations Under the New Data Security Program (DSP) for Cross-Border Operations

September 16, 2025

By: Shelley M. Jackson, Virginia A. Talley, and Marsha Jean-Baptiste

Executive Order 14117 (Prevent Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern) and its implementing regulations establish the Data Security Program (DSP), a new compliance framework that companies must navigate when transferring U.S. sensitive personal data or U.S. government-related data to foreign service providers.

On April 8, 2025, entities and individuals were required to comply with DSP's prohibitions and restrictions. Starting October 6, 2025, entities and individuals must begin compliance with the due diligence, audit, and reporting requirements for restricted transactions. While the DSP does not impose a blanket prohibition on international outsourcing or data sharing, it creates affirmative compliance obligations for U.S. companies working with foreign entities—even those located outside of “countries of concern.”

Key Takeaways for Companies with Global Operations or Outsourcing Relationships

1. Transactions With Foreign Third Parties

- The DSP generally prohibits transactions involving “countries of concern” (currently defined as China, Cuba, Iran, North Korea, Russia, and Venezuela) and “covered persons” (foreign entities/individuals substantially connected to those countries).
- Transactions with foreign third parties not tied to countries of concern are permitted, but subject to compliance safeguards.

2. Mandatory Contractual Provisions

- U.S. companies must include explicit contractual restrictions prohibiting foreign third parties from reselling or transferring data to a country of concern or covered person.

3. Reporting Obligation



- Companies must promptly report any known or suspected violations of these contractual restrictions to the Department of Justice's National Security Division (NSD).

4. Scope of Application

- Even when foreign counterparties are located in jurisdictions not designated as countries of concern, U.S. companies must implement the required controls.
- Covered data includes bulk U.S. sensitive personal data (such as health, geolocation, or financial information) and government-related data.

5. Penalties

- Individuals and entities that conspire to violate or attempt to evade the DSP's restrictions may face criminal penalties of up to 20 years' imprisonment and fines of up to \$1,000,000, as well as civil penalties of up to the greater of \$368,136 or twice the value of the transaction at issue.

Practical Compliance Recommendations

- Contract Review: Update template agreements with foreign vendors/service providers to include DSP-compliant restrictions.
- Vendor Due Diligence: Confirm that counterparties are not "covered persons" (including indirect ownership checks).
- Internal Reporting Protocols: Establish escalation procedures for identifying and reporting potential violations.
- Training & Awareness: Ensure legal, compliance, and procurement teams understand DSP obligations when structuring outsourcing or cross-border arrangements.

Conclusion

The DSP reflects the U.S. government's heightened scrutiny of bulk personal data transfers and the potential national security risks of onward transfers to adversarial states. Companies with global footprints or outsourced operations should act now to integrate DSP compliance into contract management, vendor oversight, and incident reporting processes.

For guidance on implementing these requirements in your contracts or questions about how DSP may impact your business, contact Shelley M. Jackson, Virginia A. Talley, Marsha Jean-Baptiste, or another member of Krieg DeVault's Data Privacy Team.

Disclaimer: The contents of this article should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult with counsel concerning your situation and specific legal questions you may have.