Maturing Compliance with the Bulk Sensitive Data Rule (Data Security Program) before the July 8, 2025 Safe Harbor Expires

May 28, 2025

All eyes are on the DOJ Bulk Sensitive Data Rule (28 C.F.R. Part 202) and July 8, 2025, when the recently announced good-faith safe harbor expires. The rule, which the Department of Justice now refers to as the Data Security Program (the "DSP"), creates a comprehensive export control regime to restrict the transfer of bulk sensitive personal and government-related data to foreign adversaries deemed threats to U.S. national security. On April 11, 2025, shortly after the first effective date of the DSP, the National Security Division ("NSD") of DOJ issued a suite of three policy and guidance documents to facilitate compliance with the DSP, including a 90-day civil enforcement safe harbor for good-faith compliance. As previously discussed, the DSP seeks to address the bipartisan concern that sensitive datasets could be exploited by foreign adversaries for espionage, cyberattacks, malign influence, and coercion, which would undermine the United States' national security interests.

The existing compliance deadlines are:

- **April 8, 2025**: comply with the DSP's prohibitions and restrictions relating to covered data transactions and with all other provisions of the DSP with the exception of the affirmative obligations of subpart J (due diligence and audit requirements for restricted transactions), § 202.1103 (reporting requirements for certain restricted transactions), and § 202.1104 (reports on rejected prohibited transactions).

- **October 6, 2025**: comply with subpart J and §§ 202.1103 and 202.1104.

The April 11, 2025 suite of policy and guidance documents consists of: (1) an Implementation and Enforcement Policy; (2) a Compliance Guide; and (3) a set of frequently asked questions ("FAQs"). In this blog post we will summarize these documents and highlight a few topics from each of the Compliance Guide and FAQs for further assessment as companies continue to evaluate their compliance posture vis-à-vis the DSP leading up to the end of the safe harbor period and the October 6, 2025 compliance date.

Implementation and Enforcement Policy: 90-day Civil Enforcement Safe Harbor for Good-Faith Compliance

90-Day Safe Harbor

In the Implementation and Enforcement Policy (the "Policy"), DOJ indicated that "it will not prioritize civil enforcement actions against any person for violations of the Data Security Program that occur from April 8 through July 8, 2025, so long as the person is engaging in good-faith efforts to comply with or come into compliance with the Data Security Program during that time." According to DOJ, this is so that private sector U.S. persons can have (1) additional time to implement the changes required by the DSP and (2) additional opportunities for the public to engage with NSD, generally minimizing potential disruptions for businesses as a result of the DSP.

Examples of Good-Faith Efforts Listed in the Policy

In the Policy DOJ sets out the clear expectation for U.S. persons to "know their data," including: (1) the kind and volume of data collected or maintained concerning U.S. persons; (2) how they use this data and whether they engage in covered data transactions with covered persons or countries of concern; and (3) how such data is marketed, particularly with respect to current or recent former employees or contractors or former senior officials of the United States government, including the military and U.S. Intelligence Community. DOJ also recognizes the differential compliance efforts and uplift required, which depend on the U.S. persons' existing structure and commercial activities.

DOJ provides a roadmap of compliance efforts NSD believes would demonstrate good-faith compliance efforts, including:

- Conducting internal reviews of access to sensitive personal data, including whether transactions involving access to such data flows constitute data brokerage;
- Reviewing internal datasets and datatypes to determine if they are potentially subject to the DSP;
- Renegotiating vendor agreements or negotiating contracts with new vendors;
- Transferring products and services to new vendors;
- Conducting due diligence on potential new vendors;

- Negotiating contractual onward-transfer provisions with foreign persons who are the counterparties to data brokerage transactions;
- Adjusting employee work locations, roles, or responsibilities;
- Evaluating investments from countries of concern or covered persons;
- Renegotiating investment agreements with countries of concern or covered persons; and
- Implementing the Cybersecurity and Infrastructure Security Agency ("CISA") Security Requirements, including the combination of data-level requirements necessary to preclude covered person access to regulated data for restricted transactions.

Informal Consultation Encouraged

During this time, NSD will still pursue penalties and other enforcement actions as appropriate for egregious, willful violations. While NSD will not review or adjudicate any formal requests for specific licenses or advisory opinions during this 90-day period (absent an emergency or imminent threat to public safety or national security)—and discourages submissions of the same—it encourages the public to contact NSD at nsd.firs.datasecurity@usdoj.gov with informal inquiries or information about the DSP and the guidance NSD has released.

The Compliance Guide

Clarifications re Secondary Due Diligence Obligations and Model Contractual Language for Onward Transfers

In the Compliance Guide, DOJ provides helpful guidance on certain important items under the DSP broadly, including the fact that U.S. persons are not obligated to proactively seek information or diligence their vendors' potential employment arrangements with covered persons as part of the "knowing" and "directing" analysis to determine whether their vendors' employees are covered persons. Of note, DOJ points out that "[g]enerally, absent indications of evasion, conspiracy, or knowingly directing prohibited transactions, U.S. persons that conduct adequate due diligence as part of a risk-based compliance program [that engage in data brokerage] would not have engaged in a prohibited transaction if the foreign counterparty later violates the required contractual provision or if the U.S. person fails to detect such violations."

DOJ also provides model contractual language that companies engaged in data brokerage can use when contracting with foreign persons to address prohibited onward transfers to countries of concern or covered persons. Further, DOJ adds that companies must exercise due diligence to ensure and monitor compliance with such contractual provisions prohibiting potential onward transfer to countries of concern or covered persons in order to report any rejected prohibited transaction consistent with § 202.1104.

Minimum Requirements for the Data Compliance Program for Restricted Transactions

The Compliance Guide closely tracks the DSP final rule issued in January 2025, including its summary of the key definitions, differentiation between prohibited and restricted transactions, and reiteration of various reporting and recordkeeping requirements, including the obligation for U.S. persons to maintain full and accurate records, for at least 10 years, of (1) any non-exempt covered transaction, (2) covered data transactions subject to a general or specific license, and (3) certain exempt transactions under § 202.510 for certain drug, biological product, and medical device authorizations.

Importantly, however, DOJ provides a set of minimum requirements for the design and implementation of a Data Compliance Program ("DCP"), effective as of October 6, 2025, by all U.S. persons who engage in *restricted transactions*. *Restricted transactions* are covered data transactions involving a vendor agreement, employment agreement, or investment agreement with a country of concern or covered person. While the Guide underscores that adoption of these minimum requirements will not provide a safe harbor for apparent violations of the DSP, and the failure to adopt does not per se suggest a violation, companies should expect these minimum requirements to be scrutinized closely in any potential NSD inquiries. The Guide notes that a failure to "adopt and maintain adequate data compliance policies and procedures is potentially a violation of the DSP and may be an aggravating factor in any enforcement action."

The FAQs

The FAQs also closely track the DSP final rule and issuing release but provide certain clarifications beyond the text of the rule that may merit further deep dives, including relating to, among others:

- **The scope of personal health data** is not limited to data collected only by medical and healthcare professionals and institutions, and includes, for example, logs of exercise habits collected by fitness apps.

- **The scope of personal financial data** does not include inference about financial transactions (e.g., interest in travel inferred from hotel record transactions) but includes payment history beyond just that collected by financial institutions.

- **Determination of U.S. persons**: Any covered person designated under § 202.211(a)(5) would remain a covered person wherever they are located (including while traveling to the U.S.) whereas a non-designated covered person would be considered a U.S. person while located in the United States.

- **Implications of adherence to CISA security requirements**. Deploying the security requirements to prevent a covered person's access to sensitive personal data has no bearing on whether the restricted transaction is still a covered data transaction, and the FAQs underscore that U.S. persons would still need to comply with DSP's other requirements for restricted transactions.

- **Auditor independence**: While internal audit may be used to meet the audit requirement for restricted transactions as long as they are sufficiently independent, internal auditors often lack the independence, expertise, and resources to conduct objective and thorough evaluations of their own company's compliance efforts, while external audits often provide more effective and comprehensive assessments.

- **Whistleblower incentives**: The FAQs state that "[i]ndividuals reporting violations of the DSP may be eligible for financial incentives if they do so through FinCEN's whistleblower incentive program," which covers the IEEPA, which the DSP falls under. If the information whistleblowers provide results in penalties exceeding $1,000,000, individuals may be eligible for up to 30% of those penalties. Whistleblowers are also protected by federal law from retaliation.

Takeaways

Companies should continue to use the 90-day safe harbor to assess data flows and work on their existing compliance efforts, including continued risk assessments and DCP buildout, as applicable. Companies subject to the DSP should consider:

- **Reviewing the Good-Faith Compliance Activities List** to evaluate whether any of the listed items are not already in motion and may be helpful for addressing concerns raised by the DSP;

- **Mapping Existing Compliance Roadmap Against the DCP Minimum Requirements Checklist** to identify areas of potential compliance uplift and

resource need and/or categories where existing company processes could be leveraged for efficiencies (e.g., personnel training, audit, certifications, recordkeeping);

- **Identifying Potential Synergies with Existing National Security Compliance Programs**, including with respect to the covered persons list screening, especially if software tools or third parties are implicated;

- **Monitoring for Additional Guidance** from DOJ on the DSP, including the issuance of any additional FAQs (resulting from informal consultations or otherwise) and other topical guidance; and

- **Review Existing Whistleblower Policies and Procedures** to ensure that they are consistent with federal protections. For additional guidance and practical tips, see our prior blog post on whistleblower programs.

* * *

Please do not hesitate to contact us with any questions.

Luke Dembosky
Partner, Wahington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Rick Sofield
Partner, New York
+1 202 383 8054
rcsofield@debevoise.com

Johanna N. Skrzypczyk
Counsel, New York
+1 212 909 6291
jmskrzypczyk@debevoise.com

Mengyi Xu
Associate, San Francisco
+1 415 738 5725
mxu@debevoise.com