Ready To Know Your Data? DOJ Issues Implementation and Enforcement Guidance for Data Security Program Protecting Bulk Sensitive Data

Client Alert | 6 min read | 04.18.25

On April 11, 2025, the U.S. Department of Justice (DOJ) issued guidance regarding the implementation and enforcement of the newly enacted final rule, "**Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons**," now referred to as the Data Security Program (DSP). The **release** included an **Implementation and Enforcement Policy**, a **Compliance Guide**, and **Frequently Asked Questions** (FAQs). Collectively, these documents are designed to help entities subject to the DSP understand and comply with the obligations set out under the Final Rule.

While much of the content reiterates information already established in the final rule, key insights from the newly released documents are summarized below.

What is the DSP?

The DOJ created the DSP to establish rules for U.S. persons and entities engaging in certain data transactions that the U.S. Government has determined pose an unacceptable risk of giving "countries of concern" or "covered persons" access to government-related data or bulk U.S. sensitive personal data. Among other requirements, the DSP identifies classes of prohibited and restricted transactions, identifies countries of concern and classes of covered persons to whom the proposed rule applies, identifies classes of exempt transactions, and establishes processes to issue licenses authorizing certain prohibited or restricted transactions. Unofficially, many have equated it to an export control program for the relevant data.

Limited Enforcement Policy for First 90 Days

The DSP final rule took effect on April 8, 2025, with additional compliance requirements, including due diligence, auditing, and reporting, scheduled to become effective on October 6, 2025.

Under the Implementation and Enforcement Policy, the DOJ announced a phased approach to enforcement, offering a 90-day period — from April 8 to July 8, 2025 — during which it will deprioritize civil enforcement actions for violations of the DSP, provided that entities are making "good-faith efforts" to comply with the DSP during that period. DOJ provided examples of actions that may constitute good-faith effort, including:

- Reviewing internal datasets and datatypes to determine if they are potentially subject to DSP;
- Renegotiating vendor agreements or negotiating contracts with new vendors, or transferring products and services to new vendors;
- Adjusting employee work locations, roles or responsibilities;

- Evaluating investments from countries of concern or covered persons;
- Implementing the Cybersecurity and Infrastructure Agency ("CISA") Security Requirements, including the combination of data-level requirements necessary to preclude covered person access to regulated data for restricted transactions.

However, DOJ reserves the right to pursue enforcement action for "egregious, willful violations" even during the 90-day window, and states that it expects entities to be "in full compliance" with the DSP at the end of the 90 days.

"Know Your Data" Requirements

The FAQs and Compliance Guide explain that entities subject to the DSP must develop and implement "know your data" compliance programs to verify data transactions, including the nature and volume of data, how the data is used, and how the data is marketed. However, FAQ 80 clarifies that entities are not expected to decrypt or aggregate data in their possession to comply with the Rule's "know your data" standard. This explanation is aligned with the DSP final rule's explanation that cloud service providers will not be expected to "know" their customers' encrypted data to comply with DSP.

Health Data

As discussed in our **previous analysis**, the DSP has significant implications for companies dealing with bulk sensitive personal health and human 'omic data, necessitating a thorough understanding of the scope and definition of such data.

While the compliance documents largely reiterate the health data-relevant definitions set out in the DSP final rule, FAQ 31 clarifies the scope of personal health data, indicating that it is not solely limited to information collected by healthcare providers or institutions. Rather, it includes any data that meets the definition, regardless of who collects it or in what context. This broader definition is significant because it extends beyond the parameters set by the Health Insurance Portability and Accountability Act (HIPAA), which links health information to the type of entity managing it.

CISA Requirements

The FAQ and Compliance Guidance confirm that restricted transactions—*i.e.*, bulk data transactions that would otherwise be prohibited—can be authorized if CISA's "**Security Requirements for Restricted Transactions**" are implemented to mitigate the risk of in-scope data access by countries of concern or covered persons. But FAQ 68 cautions that adherence to the CISA requirements alone does not provide blanket coverage, explaining that entities will need to take additional steps as required by the DSP for the restricted transaction to proceed (e.g., maintain a due diligence program for restricted transactions).

DSP vs. PADFAA

FAQ 12 provides an overview of the distinction between the DSP and the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFAA), a law that makes it unlawful for data brokers to sell U.S. persons' sensitive data to foreign adversaries. Key differences identified in FAQ 12 include:

- PADFAA covers a broader array of data types than the DSP, including U.S. individual's photos, videos, and other private communications.
- PADFAA applies only to the activities of third-party "data brokers," while the DSP applies to all U.S. entities that engage in covered transactions.
- While both PADFAA and the DSP restrict transactions involving China, Russia, North Korea, and Russia, the DSP also includes Venezuela and Cuba as countries of concern. Though not noted in the FAQ, DSP also expressly includes Hong Kong and Macau, while PADFAA is limited to just Mainland China.

Exemption for U.S. Government Official Business

FAQ 73 clarifies that the exemption for covered data transactions conducted pursuant to a grant, contract, or other agreement with U.S. federal government departments and agencies applies even if the transaction also involves some funding from non-federal entities. However, DOJ also notes that the exemption applies only if the relevant federal grant or contract directs or authorizes the covered data transaction.

No Cookie-Cutter Compliance Programs

The FAQs reiterate in several places that there is no one-size-fits-all compliance program for the DSP. Rather, each organization will need to assess its own risk profile, considering factors such as its size, sophistication, offerings, third party partners, and geographic footprint. That said, the Compliance Guide is intended to help organizations understand how to navigate those considerations. This is also consistent with the CISA Requirements, which demands a risk assessment to determine appropriate mitigation measures to prevent access to covered data.

Key Takeaways

The DOJ's phased approach to enforcement will be much welcomed. Many organizations have been anxious that their active preparations for the DSP's effective date were uninformed by anticipated guidance that, up until last week, was unavailable. Now with that guidance in hand, those subject to the DSP should review the DSP Implementation and Enforcement Policy, a Compliance Guide, and FAQ in full, and use these documents as a reference in implementing their DSP compliance regimes. As part of that process, organizations should also document their "good faith efforts" to implement the DSP requirements so that they can take full advantage of the DOJ's 90-day soft enforcement period and mitigate the risk of alleged noncompliance.

Contacts

Kate M. Growley
Crowell Global Advisors Director
kgrowley@crowellmoring.asia

Caitlyn Weeks
Crowell Global Advisors Associate Consultant
Washington, D.C. (CGA) D | +1.202.654.2762
cweeks@ccrowellglobaladvisors.com

Jacob Harrison
Associate
He/Him/His

Washington, D.C. D | +1.202.624.2533
jharrison@crowell.com

Nigel Cory
Crowell Global Advisors Director
Washington, D.C. (CGA) D | +1.202.654.6753
ncory@crowellglobaladvisors.com

Linda Malek
Partner & CHS Managing Director
New York D | +1.212.803.4069
lmalek@crowell.com

Jodi G. Daniel
Partner & CHS Managing Director
She/Her/Hers

Washington, D.C. D | +1.202.624.2908
jdaniel@crowell.com