JENNER & BLOCK

Client Alert: New Rules for Data Flows Take Effect: What You Need to Know

News

April 17, 2025
By: Madeleine Findley, Shoba Pillay, Aaron R. Cooper, Julianna St. Onge, Alexander R.P. Ramsey

Introduction

On April 8, 2025, the United States Department of Justice's (DOJ) National Security Division's (NSD) final rule (Final Rule)[1] regulating certain sensitive US data transfers took effect. DOJ has made clear that it will take steps to enforce these regulations. Fortunately, entities seeking to understand their obligations under the Final Rule can benefit from an additional 90-day period to come into compliance.

The Final Rule, which implements Executive Order 14117[2] prohibits or restricts US persons from engaging in certain commercial transactions involving US government-related and Americans' bulk sensitive personal data involving six "countries of concern" and individuals linked to those countries or "covered persons." In connection with associated security regulations adopted by the Cybersecurity and Infrastructure Security Agency (CISA), the Final Rule establishes a Data Security Program (DSP) that applies to a variety of entities in a variety of contexts. DOJ has made clear that it intends to follow through with enforcement of the DSP given national security concerns around certain foreign countries' access to sensitive data.

On April 11, 2025, NSD issued an Implementation and Enforcement Policy along with a Compliance Guide and responses to a list of Frequently Asked Questions (FAQs). Critically, for organizations currently assessing whether the Final Rule covers their data transactions and how to respond, the Implementation and Enforcement Policy provides a de facto 90-day grace period until July 8, 2025 for coming into compliance with the DSP. During that time, NSD will not prioritize civil enforcement actions for violations of the DSP, so long as the potential enforcement target is making good-faith efforts to come into compliance. However, NSD will still pursue willful, egregious DSP violations. Covered persons should be mindful of the limited timeframe to accomplish DSP compliance and use the Compliance Guide and FAQ as reference.

The DSP: A New Compliance Regime

The DSP, first proposed in early 2024, establishes a new national security program that prohibits certain data transactions and restricts others, backed by civil and criminal penalties. The DSP largely mirrors the 2024 proposed rule described in a previous client alert, covering a wide array of entities and a broad range of data transactions, including transfers in connection with data brokerage transactions, vendor agreements, employment agreements, and investment agreements. The DSP applies to all US persons engaged in a "covered data transaction" with covered foreign persons.[3] A "covered data transaction" can involve either "US government data" or "bulk US sensitive personal data."[4]

When such a covered data transaction involves "data brokerage", *i.e.*, a sale, license, or similar commercial transaction, the transaction is prohibited.[5] Transactions made pursuant to a vendor agreement, employment agreement, or investment agreement are "restricted," and allowed if security requirements issued by CISA and other regulatory conditions are met.[6]

Key aspects of the DSP include:

- Bulk US sensitive personal data includes personal identifiers, precise geolocation data, biometric identifiers, human genomic data, and personal health data.[7] The "bulk" threshold for each category of data varies according to its perceived sensitivity.[8]
- Sensitive personal data that meets the bulk threshold is still subject to the DSP *even if it is anonymized, pseudonymized, de-identified, or encrypted*.[9] "Restricted" data transfers may nonetheless be approved if they adhere to CISA's cybersecurity requirements.
- Covered foreign persons include: (1) foreign entities headquartered in or organized under the laws of a country of concern; (2) foreign entities 50% or more owned by a country of concern or covered person, (3) foreign individuals primarily resident in a country of concern; (4) foreign individuals who are employees or contractors of a covered person, entity, or a country-of-concern government; and (5) persons publicly designated as covered by the Attorney General.[10]
- NSD may issue general or specific licenses to engage in restricted or prohibited transactions. A general license is self-executing and authorizes a particular class of otherwise prohibited transactions. A specific license authorizes a particular transaction. NSD has indicated that there will be a "presumption of denial" for specific license applications in the absence of a showing of imminent threats to public safety or national security.[11]

Implementation of the DSP is not straightforward and requires parsing a series of complex regulatory definitions. Companies subject to the DSP should take advantage of DOJ's recently issued 90-day enforcement policy to promptly develop and implement a compliance program prior to July 8, 2025, including:

- conducting internal reviews of access to sensitive data and whether they potentially constitute commercial data transactions subject to the DSP;
- reviewing internal data sets and data flows that may be subject to the DSP;
- revising or creating new internal policies and processes;
- conducting due diligence on vendors and negotiating or renegotiating vendor agreements;
- negotiating onward transfer agreements with foreign counterparties;
- reviewing corporate locations and adjusting employee roles or responsibilities;
- evaluating investments from countries of concern or covered persons;
- renegotiating investment agreements with entities from countries of concern or covered persons; and
- implementing the CISA Security Requirements.

As an initial step, all potentially covered US persons should take steps to "know their data," including the kinds and volumes of data collected about US persons and devices, how their company uses the data, and how that data is marketed, especially data of current and former US government employees and contractors and Americans' bulk sensitive personal data.[12]

Key Takeaways

The DSP represents a complex compliance regime for persons and entities that seek to transact with US data. While welcome, the NSD's 90-day grace period will pass quickly as companies work through updating compliance programs and implementing the full set of requirements under the DSP. The Compliance Guide and FAQ offer valuable guidance to assist companies with targeting their risk assessment and implementation efforts, and the continued focus on American data security suggests active enforcement to come.

Jenner & Block will continue to monitor developments and provide updates as NSD issues further guidance and begins to enforce this new data transaction regulatory regime. Persons to whom the DSP may apply should seek counsel early in their compliance efforts to identify relevant data transactions and relevant risks.

Footnotes

[1] *Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons*, 90 Fed. Reg. (Apr. 8, 2015) (codified at 28 C.F.R. Pt. 202) ("Data Security Program").

[2] Exec. Order No. 14,117, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, 89 Fed. Reg. 15421 (Feb. 28, 2024).

[3] *Data Security Program: Compliance Guide*, U.S. Dep't of Justice, Nat'l. Sec. Div., at 3 (Apr. 11, 2025) https://www.justice.gov/opa/media/1396356/dl.

[4] Data Security Program, 28 C.F.R. § 202.210(a).

[5] 28 C.F.R. § 202.301(a).

[6] 28 C.F.R. § 202.401(a).

[7] 28 C.F.R. § 202.206.

[8] 28 C.F.R. § 202.205.

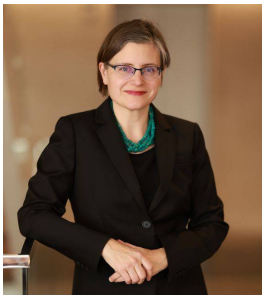
[9] 28 C.F.R. § 202.206 (emphasis added).

[10] 28 C.F.R. § 202.211.

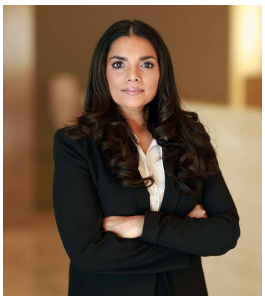
[11] *Data Security Program: Frequently Asked Questions*, U.S. Dep't of Justice, Nat'l. Sec. Div., at 40 (Apr. 11, 2025) https://www.justice.gov/opa/media/1396351/dl ("FAQs").

[12] *Id.* at 12, n.18.

Related Attorneys



Madeleine Findley
Partner
mfindley@jenner.com
+1 202 639 6095



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605

Aaron R. Cooper
Partner
acooper@jenner.com
+1 202 637 6333

Julianna St. Onge
Associate
jstonge@jenner.com
+1 312 840 7368

Alexander R.P. Ramsey
Associate
aramsey@jenner.com
+1 415 293 5953

Related Capabilities

Data Privacy and Cybersecurity

Stay Informed →