Davis Polk

DOJ releases guidance on Data Security Program

April 24, 2025 | Client Update | 8-minute read

The DOJ has published an enforcement policy and various guidance on its final rule restricting sensitive data transfers to countries of concern, including China.

On April 11, 2025, the National Security Division (NSD) of the Department of Justice (DOJ) issued a press release and multiple guidance documents on its final rule on "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons" (28 C.F.R. Part 202). As discussed in our previous update, the final rule—which NSD now calls the "Data Security Program" (DSP)— reflects a concern by both the Biden administration and the Trump administration that countries of concern, including China, could (or already do) use sensitive data to undermine national security by identifying vulnerabilities, conducting espionage or exposing U.S. citizens and officials to manipulation and blackmail (see our previous updates here and here). The DSP imposes restrictions on the ability of U.S. persons to engage in a wide range of data transactions involving vendors, employees, or customers based in or owned by "countries of concern" (most importantly, China)—including a U.S. company's own affiliates—as well as significantly restricting investment by Chinese and other investors in U.S. companies that hold significant quantities of data.

Although the due diligence, reporting and auditing processes required by the rule do not become effective until October 6, 2025, all other obligations under the rule went into effect on April 8, 2025. As we highlighted previously, ambiguities in the rule pose challenges for business seeking to adhere to requirements affecting a wide range of commonplace and crucial transactions, including preexisting contracts and arrangements as well as new agreements. Recognizing that determining whether the DSP's prohibitions and restrictions apply and implementing compliant policies may require "a number of steps," NSD published an Implementation and Enforcement Policy, which among other things provides an additional 90 days for full compliance with the NSD for businesses engaged in good faith efforts to comply.

Additionally, NSD published a Compliance Guide and answers to frequently asked questions. The Compliance Guide provides guidance on key definitions, prohibited and restricted transactions, and requirements for building a robust data compliance program. The FAQs provide high-level clarifications regarding the Executive Order that directed DOJ to issue the DSP, as well as information about the Data Security Program's scope, exemptions, and accompanying processes. The new guidance does not, however, significantly clarify the ambiguities of the final rule, largely providing a reorganized presentation of previously available information.

Background

The DSP aims to prevent "countries of concern" from accessing U.S. government-related data and Americans' bulk sensitive personal data, including geolocation, biometric, genomic, health, financial and certain personally identifying information (collectively, covered data). These countries include China, Russia, Iran, North Korea, Cuba, and Venezuela. The rule prohibits transactions by U.S. companies in which sufficient quantities of sensitive personal data are transferred to companies or individuals linked to the countries of concern (covered persons), and likewise prohibits U.S. persons from directing others to engage in such transactions. It also conditions a range of employment, investment, and procurement transactions with covered persons on compliance with a series of cybersecurity requirements released in parallel by the Cybersecurity & Infrastructure Security Agency (CISA).

The DSP combines strict bans on certain kinds of transactions with more flexible restrictions on others. It prohibits (i) U.S. persons from knowingly engaging in data brokerage transactions, or other transactions involving transfers of covered data, with covered persons, and (ii) U.S. companies that hold any significant quantity of human genomic data of U.S. persons from knowingly engaging in investment, employee, or vendor relationships with the potential to provide access to a covered person. The rule also only permits U.S. persons and companies to engage in investment, employment, or vendor agreements with the potential to provide access to such data to covered persons (restricted transactions) if they meet CISA's data security requirements.

Copyright 2025 Davis Polk & Wardwell LLP

The rule does not contain any exemptions for preexisting contracts, meaning that it affects continued access to sensitive data under current vendor, employment, and commercial relationships. However, an otherwise restricted investment agreement is exempted from the rule's data security requirements where the investment is in publicly traded securities of the issuer, amounts to a total of less than 10 percent of the U.S. business, and is completely passive.

In its most recent announcement, DOJ described the "continued prioritization" of the DSP—developed under the Biden administration—as consistent with the Trump administration's promises and goals. In particular, DOJ stated that prioritizing the DSP will help support President Trump's efforts to curb predatory investments by foreign adversaries and that the DSP addresses threats identified in the U.S. intelligence community's 2025 Annual Threat Assessment. That said, DOJ has postponed complete enforcement of the DSP in several key ways, as discussed below.

The Enforcement Policy

DOJ explained in its most recent announcement that it has decided to "provide additional time for entities and individuals to come into compliance" with the DSP. For this reason, the Enforcement Policy delays certain aspects of DSP compliance.

Good faith safe harbor

While compliance with the DSP is required as of April 8, 2025, the Enforcement Policy states that DOJ will limit its enforcement efforts during the first 90 days to allow U.S. persons to implement any necessary changes to comply with the DSP. In that spirit, DOJ will not prioritize civil enforcement actions for violations of the DSP that occur between April 8 and July 8, 2025, so long as the person or company is engaging in good faith efforts to come into compliance with the DSP during that time. The Enforcement Policy lists several practical ways that companies can demonstrate good faith 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 data types to determine if they are potentially subject to the DSP.
- Renegotiating vendor agreements or negotiating contracts with new vendors.
- Transferring products and services to, and conducting due diligence on, new vendors.
- Negotiating contractual transfer provisions with foreign counterparties to data brokerage transactions.
- Adjusting employee work locations, roles, or responsibilities.
- Evaluating investments from, and renegotiating investment agreements with, countries of concern or covered persons.
- Implementing the CISA Security Requirements, including the combination of data- and system-level requirements necessary to preclude covered person from accessing covered data.

Moreover, as a reminder, certain due diligence, audit, and reporting requirements are not effective until October 6, 2025. Delayed requirements include (i) the need to establish and annually certify a written data compliance program with risk-based procedures for verifying data flows involved in restricted transactions and for verifying the identity of the vendors involved in such transactions; (ii) the need to conduct annual audits of all restricted transactions and of the data compliance program; and (iii) the obligation of the auditor to submit detailed reports to the person engaging in the restricted transactions, and of that person to retain each report for a 10-year period.

The Compliance Guide and FAQs

DOJ also issued a detailed Compliance Guide and FAQs alongside the Enforcement Policy. The Compliance Guide provides summaries of key definitions, prohibited and restricted transactions, reporting requirements with respect to suspected or attempted violations, and requirements for building a robust data compliance program. It also provides model contractual language and best practices for complying with the Data Security Program's audit and recordkeeping requirements. Further, it explains in detail that U.S. individuals and entities should "know their data." Though many aspects of the compliance program's design as described in the Compliance Guide will be familiar to sophisticated companies, explicitly keying compliance activities to these recommendations may prove useful should a company's program ever come under scrutiny.

The FAQs, meanwhile, provide high-level summaries of the Executive Order that directed DOJ to issue the DSP, as well as information about the Data Security Program's scope, exemptions, and accompanying processes, such as requesting

Copyright 2025 Davis Polk & Wardwell LLP

licenses and advisory opinions, disclosing violations, and reporting rejected prohibited transactions. The FAQs largely repeat information available in the final rule adopting the DSP.

Penalties

Noncompliance with the rule, material misstatements or omissions in connection with reporting and other requirements of the rule, false certifications or submissions, or other violations would be subject to a civil penalty not to exceed the greater of $368,136 per violation or an amount that is twice the amount of the transaction that is the basis of the violation. Willful violations can result in criminal penalties, such as a fine of up to $1 million or imprisonment of up to 20 years.

Next steps

Companies should use the Enforcement Policy's 90-day "good faith" safe harbor to conduct risk assessments and take steps to ensure compliance. Companies should consider:

— Completing an inventory of their existing data to determine whether they maintain covered data.

— Mapping existing governance structures, policies, and procedures onto the DSP's compliance recommendations.

— Reviewing the sample contractual clauses included in the Compliance Guide to inform amendments or negotiations with new vendors.

— Monitoring for new developments. For example, the FAQs note that companies should expect further guidance from the NSD, including regarding mitigating factors, the requirements for a sufficiently independent audit, and NSD's general framework for enforcement of the DSP. NSD has also signaled that it plans to take an approach to voluntary disclosure that aligns with the U.S. Export Administration Regulations, which call for an initial notification followed by a full report within six months.

— Preparing to seek advisory opinions and licenses, if necessary. The NSD specified that companies should consider waiting until after the 90-day pause to apply for such advisory opinions and licenses, and that such requests will be reviewed under a "presumption of denial."

— Generally proceeding with urgency. A 90-day enforcement pause is not much time for companies to ingest this new guidance, especially those that interact with sensitive data types or do business in covered countries.

Copyright 2025 Davis Polk & Wardwell LLP

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Matthew J. Bacal
+1 212 450 4790
matthew.bacal@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

David I. Feinstein
+1 212 450 3293
david.feinstein@davispolk.com

James W. Haldin
+1 212 450 4059
james.haldin@davispolk.com

Neil H. MacBride
+1 202 962 7035
neil.macbride@davispolk.com

Paul D. Marquardt
+1 202 962 7156
paul.marquardt@davispolk.com

Martin Rogers
+852 2533 3307
martin.rogers@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com

Miranda So
+852 2533 3373
miranda.so@davispolk.com

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.

Copyright 2025 Davis Polk & Wardwell LLP