JENNER & BLOCK

Client Alert: Myth Busters: Dispelling Common Misconceptions of the Department of Justice's Data Security Program

Publications

May 12, 2025
By: Aaron R. Cooper, Nikita Lalwani

A month has passed since the Department of Justice (DOJ) National Security Division's (NSD) issued its Final Rule prohibiting certain transactions involving US government data and Americans' bulk sensitive personal data. Designed to prevent foreign adversaries from accessing and exploiting data that could be used to enhance artificial intelligence capabilities, augment intelligence collection and foreign espionage, and enable malicious cyberattacks and malign foreign influence capabilities, the Final Rule sweeps broadly across the private sector.

But misconceptions about the Final Rule—including five common ones below—could lead many to mistakenly believe their activities are outside its scope. Fortunately, on April 11, DOJ issued a delayed enforcement policy allowing 90 days for organizations to come into compliance. Before the grace period expires on July 8, organizations should proactively assess how their data flows interact with the Final Rule's provisions and, if necessary, implement new compliance regimes to meet its requirements.

Myth #1: The rule applies only to data brokers. I am not a data broker, so the rule does not apply to me.

Wrong! *The rule is not directed at a particular industry. It applies to any US firm or natural person that engages in a "covered data transaction," which encompasses a range of commercial activities.* A covered data transaction is a transaction involving data brokerage, a vendor agreement, an employment agreement, or an investment agreement that allows a country of concern or a covered person to gain access to any government-related data or bulk US sensitive personal data. (Sensitive personal data includes certain personal identifiers, precise geolocation data, biometric identifiers, human "omic" data, personal health data, and personal financial data.)

Different kinds of transactions are subject to different rules. Transactions involving data brokerage—such as the sale of data or the licensing of access to data, which are activities that are not limited solely to data brokers—are subject to the most stringent prohibitions: US persons may not knowingly engage in such a transaction with a country of concern (China, Cuba, Iran, North Korea, Russia, or

Venezuela) or with a covered person (certain foreign companies and foreign individuals located in a country of concern). Vendor, employment, and investment agreements with covered persons, meanwhile, are prohibited unless the US person complies with a robust set of security requirements to ensure the safety of sensitive US data, plus due diligence, audit, and record-keeping requirements. Those requirements include cybersecurity policies, physical access controls, and the application of various encryption techniques, among other provisions available here.

Myth #2: I can easily anonymize, de-identify, encrypt, or aggregate data to avoid the rule. So I have nothing to worry about.

It's not so simple! *A "covered data transaction" includes bulk US sensitive personal data regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted—but the restrictions on such transactions depend on whether they involve data brokerage or vendor, employment, or investment agreements.* If the transaction involves data brokerage, there is a flat prohibition on US persons knowingly engaging with a country of concern or with a covered person. If the transaction involves vendor, employment, or investment agreements, however, the activities may proceed if companies meet certain security requirements, including, as relevant here, the use of data-protection techniques such as aggregation, pseudonymization, de-identification, and anonymization. Note, however, that companies wishing to proceed with such agreements must also meet a host of other organizational, system-level, and data-level requirements—for example, designating a chief information security officer, conducting internal data-risk assessments, and maintaining and implementing a written data retention and deletion policy, plus meeting due diligence, audit, and record-keeping requirements.

Myth #3: I deal only with foreign companies that are not covered persons under the rule, so I'm not subject to its requirements.

Not so fast! *If you are engaged in covered data transactions with a foreign person that is not a covered person, you must have in place contractual commitments to protect the risks of onward transfer of that data to a covered person*. Most of the rule is targeted at transactions with "covered persons," a category that includes foreign companies that are 50% or more owned by countries of concern, foreign individuals that are employees or contractors of such companies, and foreign individuals that live in a country of concern. So, analysis of foreign company ownership is paramount. But the rule also includes restrictions on transactions with foreign persons that are not covered persons: for example, a Dutch company with no ties to China, Cuba, Iran, North Korea, Russia, or Venezuela. US persons may not knowingly engage in a covered data transaction involving data brokerage with such persons unless the US person (1) contractually requires that the foreign person refrain from onward sale with a country of concern or covered person; and (2) reports any known or suspected violations of this contractual requirement.

Myth #4: I already have data privacy and export control compliance programs in place. I can just rely on those programs to satisfy the rule.

No! *Given the rule's distinct provisions, companies will benefit from a tailored compliance effort—including the potential implementation of specific due diligence, audit, and record-keeping requirements.* Although the program has some similarities to both data privacy and export control regimes—it regulates sales of sensitive personal data to foreign persons, for example, and allows entities to apply for specific licenses—it also has its own complex set of definitions and requirements. By October 6, 2025, for example, US persons engaging in any restricted transactions must develop and implement a data compliance program that includes procedures for verifying and logging data flows, procedures for verifying the identity of vendors, an annually certified written data compliance policy, and an annually certified policy describing the implementation of the rule's security requirements. In addition, US persons engaging in any transactions subject to the rule must keep "a full and accurate record of each such transaction" available for at least 10 years after the transaction date and make those records available to DOJ upon request. These provisions, among others, suggest that companies should start investing now in proactive and ongoing compliance efforts specific to the rule.

Myth #5: The DOJ won't actually enforce the rule, so I shouldn't be too concerned about risk.

No! *The DOJ's leadership has been clear that it will prioritize enforcement of the rule.* In a press release announcing the rule, the DOJ characterized the program as consistent with multiple Trump Administration policies, including President Trump's America First Investment Policy, National Security Presidential Memorandum-2 on Imposing Maximum Pressure on Iran, the 2025 Annual Threat Assessment of the US Intelligence Community, and the 2017 National Security Strategy. Underscoring the importance of the rule, Deputy Attorney General Todd Blanche promised that the program would make it "a lot harder" for foreign adversaries to "get Americans' data."

The DOJ has also taken the time to issue a compliance guide, a list of more than 100 Frequently Asked Questions, and an implementation and enforcement policy. That policy explains that "prompt compliance with the [program's] requirements is critical to addressing the Administration's priorities," and urges companies to take steps to "know their data," including whether they engage in covered data transactions with covered persons or countries of concern. Although the DOJ will not prioritize civil enforcement for rule violations that occur during the 90-day grace period, it will "pursue penalties and other enforcement actions as appropriate for egregious, willful violations," and it retains the discretion to pursue civil enforcement if firms do not engage in good-faith efforts to come into compliance.

Companies should therefore act now to assess their obligations under the rule and engage in good-faith compliance efforts, for example by conducting internal reviews of access to sensitive personal data, renegotiating vendor agreements, adjusting employee work locations or responsibilities, or implementing relevant security requirements. Once the grace period expires, violators will be subject to steep civil and/or criminal penalties, including up to 20 years in prison, under the International Emergency Economic Powers Act.

Related Attorneys

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

Nikita Lalwani
Associate
nlalwani@jenner.com
+1 202 639 6021

Related Capabilities

Critical and Emerging Technologies

Data Privacy and Cybersecurity

Stay Informed →