Proskauer

DOJ Begins Enforcement of New Data Security Program

Minding Your Business on **July 21, 2025**

On July 9, 2025, the Department of Justice ("DOJ") commenced enforcement of its new Data Security Program ("DSP") to prevent foreign adversaries from accessing sensitive U.S. data. Created earlier this year, the program seeks to prevent China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela (collectively, the "Countries of Concern"), as well as foreign entities or individuals with significant ties to these nations, from gaining access to U.S. government-related data and certain categories of U.S. sensitive personal data. Importantly, the rules apply "regardless of whether the data is anonymized, pseudonymized, de-identified or encrypted." According to the DOJ, the threat of foreign adversaries collecting and weaponizing U.S. data had become "increasingly urgent, and ensuring prompt compliance with the DSP's requirements is critical to addressing the administration's priorities and stopping the flow of U.S. sensitive personal data and government-related data to countries of concern." The seriousness of any infraction is reflected in the program's steep civil and criminal penalties. Violators of the DSP could be subject to fines up to $368,136 per violation, or twice the value of each transaction in violation, whichever is greater. Willful violators could face imprisonment of up to 20 years and a $1 million fine.

The DSP officially went into effect on April 8, but to assist the public in complying with the new program, the DOJ has since provided various resources, including a Compliance Guide and an initial list of Frequently Asked Questions. Notably, the DOJ also provided for a 90-day pause in civil enforcement of the DSP for companies working in good faith to comply with the program. This hiatus officially concluded on July 8.

Given the DOJ's commitment to providing extensive guidance on the new program, and implementing an enforcement pause to allow the public to learn and comply with the accompanying new rules, enforcement of the DSP is expected to be strict. Although the DOJ is looking for "willful" violations, a relatively high standard for the government, ample available guidance makes it hard for defendants to argue that one was unaware or not knowingly violating the rule. Delays in addressing noncompliance or ignoring noncompliance can also evidence a willful violation. In fact, the DOJ cautioned that "individuals and entities should be in full compliance with the DSP and should expect [the DOJ's National Security Division ("NSD")] to pursue appropriate enforcement with respect to any violations."

The program is likely here to stay. The DSP originates from one of few Biden-era executive orders that the second Trump administration has prioritized; this largely bipartisan effort shows an enduring commitment to addressing national security concerns and implementing rules on operating with foreign adversaries. Moreover, the program aligns with several recent moves by the DOJ that demonstrate an increased focus on achieving President Trump's "America First" agenda. For example, the DOJ in parallel revealed a revised white-collar enforcement strategy that emphasized "America First" administrative principles, including prioritizing cases involving foreign adversaries and foreign companies harming U.S. interests. Similarly, the DOJ resumed FCPA enforcement with a new "America First" lens, focusing on cases that undermine U.S. national interests to safeguard U.S. national security. The DSP also cites to President Trump's "America First" policy – reinforcing the DOJ's heightened priority to bring and enforce violations that threaten U.S. national security.

What to do now? The program is broad in scope and regulates data transactions through a framework that deviates significantly from existing data privacy protection laws. U.S. companies that conduct international data transactions should be particularly cognizant of the new program's requirements. Organizations should assess their data-sharing and receiving practices and avoid transactions prohibited under the DSP. Companies and individuals should also be mindful that the program's compliance obligations will continue to expand; additional due diligence, audit, and reporting requirements will take effect on October 6, 2025. Given the government's commitment to ensure compliance (and rebut ignorance of the new program), companies and individuals should keep a close eye on additional guidance from NSD and continue to implement best practices for data security.

View original.

Related Professionals

- **Emma K. Baker**
  Associate