U.S. Justice Department Establishes New Data Security Program to Prevent Foreign Adversaries from Exploiting Americans' Sensitive Data

Client Advisories

06.23.2025

By: Kate A. Sherlock, Jiyoung Won

U.S. companies that collect and store sensitive personal data have until July 8, 2025 to comply with a new Department of Justice rule, known as the **Data Security Program** ("DSP").

What is the Data Security Program?

The DSP prohibits U.S. companies from sharing bulk sensitive personal data with individuals or entities from countries identified as foreign adversaries, including but not limited to China, Russia, Cuba, Venezuela, and Iran ("Covered Person(s)"). Under the program, sensitive personal data is defined broadly and is not limited to traditional "PII", such as social security numbers and bank account information. Instead, the DSP aims to protect a much broader scope of information, including but not limited to human genomic information, geolocation information, biometric and health information, and financial information. Additionally, the DSP applies to government-related data, including any precise geolocation data and sensitive personal data that a transacting party markets as linked or linkable to certain current or recent former U.S. government employees.

The new rule creates data export restrictions to prevent foreign adversaries from gaining access to large amounts of sensitive data. Certain types of transactions are prohibited under the DSP, including but not limited to data brokerage agreements with a Covered Person involving bulk U.S. sensitive data or government data without a valid license.

Why Was the DSP Created?

The Department of Justice established the DSP to protect U.S. national security against foreign adversaries seeking to weaponize Americans' sensitive data.

What Are the Penalties?

The DSP is implemented by the National Security Division (NSD) pursuant to Executive Order 14117. Violators may face civil and, in some cases, criminal penalties including fines of up to $1 million and prison terms of up to 20 years. While the new rule went into effect on April 8, 2025, the NSD has indicated it will prioritize compliance over enforcement during the initial 90-day period. Certain affirmative due-diligence obligations are delayed and will not take effect until Oct. 6, 2025.

To support compliance efforts, the NSD has published a Compliance Guide, over 100 FAQs, and will publish a Covered Persons List identifying persons subject to the control and direction of foreign adversaries.

What Should Companies Do to Comply?

Companies should immediately review internal datasets to identify any data that constitutes sensitive personal data under the new rule. Companies that hold sensitive personal data should then evaluate whether such data meets the bulk thresholds established in the rule, which vary depending on the data type at issue. Companies should also review whether they possess government-related data, which is subject to heightened scrutiny.

If regulated data is identified, companies should determine whether they are engaged in any restricted transactions under the DSP and, if so, whether they must meet certain compliance requirements to lawfully proceed with such transactions.

Companies with regulated data should also review whether they are engaged in data brokerage arrangements with individuals and entities from non-adversarial foreign countries ("Non-Covered Person(s)"). Under the rule, companies with regulated data may engage in data brokerage agreements with Non-Covered Persons only if certain conditions are met, such as contractually restricting the Non-Covered Person from reselling or giving a Covered Person access to regulated data.

Organizations should consider implementing a full data compliance program, including written policies, employee training, due diligence, and regular audits to assess risk, meet security requirements, and manage transactions and relationships where regulated data may be shared.

In addition to the resources noted above, companies may submit informal compliance inquiries to the Department of Justice at nsd.firs.datasecurity@usdoj.gov prior to the July 8 enforcement start date. After that point, companies are expected to be in full compliance with the rule, and violations may result in civil and/or criminal penalties.

Next Steps

If you need assistance evaluating your business's compliance with the DSP or have questions about the issues discussed in this advisory, please contact Kate Sherlock at ksherlock@archerlaw.com or Jiyoung Won at jwon@archerlaw.com.

DISCLAIMER: This client advisory is for general information purposes only. It is a summary, not a full analysis, of the topic. It is not intended, and should not be construed, as legal advice, and may not be used or relied upon as a substitute for legal advice by a qualified attorney regarding a specific matter. It may be considered an advertisement for certain purposes.

Related People

Kate A. Sherlock

Partner

ksherlock@archerlaw.com

856.673.3919

Jiyoung Won

Associate

jwon@archerlaw.com

201-498-8557