# PUBLICATION

## DOJ Final Rule Casts Wider Net: Common Business Data May Now Trigger National Security Scrutiny

**Authors: Vivien F. Peaden**
**June 05, 2025**

**If you thought your company's collection of email address, IP address, zip code, birth date, or cookie data was too mundane to catch the federal government's attention – think again. Effective April 8, 2025, a new DOJ final rule prohibits or restricts access to U.S. bulk sensitive personal data and U.S. government-related data by certain countries of concern, such as China (encompassing Hong Kong and Macau).**

Although framed as a national security safeguard, the Data Security Program (DSP) requires all U.S. companies to conduct due diligence when engaging in commercial transactions involving the data transfer to foreign entities. Even everyday data points, in combination with another data point known as **"Listed Identifiers"**, can become sensitive personal data, creating potential national security risks that the DSP aims to mitigate. Although the DOJ has indicated it will not prioritize civil enforcement actions for violations of the DSP occurring between **April 8 and July 8, 2025, this period is not a grace period** – U.S. businesses must remain vigilant, as enforcement can still occur if a company does not engage in good faith compliance efforts, such as amending or renegotiating existing contracts, conducting internal reviews of data flows, deploying the CISA security requirements.

### 1. Routine Business Data becomes Sensitive under the DOJ Rule when in combination with other linkable identifiers

At the heart of the DOJ Rule is the concept of "bulk U.S. sensitive personal data", referring to "a collection or set of sensitive personal data of U.S. person, in any format, where such data meets or exceeds the applicable bulk threshold " outlined in the DOJ Rule. Notably, the DSP does not exempt sensitive personal data even if it has been anonymized, pseudonymized, de-identified, or encrypted (as highlighted in our prior alert).

The term "**sensitive personal data**" under the DOJ Rule extends beyond traditionally regulated personal data categories to include not only classic data types, such as precise geolocation data, biometric identifiers, human ' omic data, personal health data, and personal financial data, but also "**covered personal identifiers**", referring to one "**Listed Identifier**" in combination with another covered identifier.

The DSP purposefully provides a broad definition for "**Listed Identifier**" that includes seemingly routine data identifiers collected and processed in everyday business operations. The enumerated Listed Identifiers are:

(a) **Government IDs**, referring to a Social Security number, driver's license or State ID, passport number, or Alien Registration Number);

(b) **Financial account info**, referring to full financial account numbers or personal identification numbers associated with a financial institution or financial services company;

(c) **Device Identifiers**, referring to International Mobile Equipment Identity (**IMEI**), Media Access Control (MAC) address, or Subscriber Identity Module (SIM) card number;

(d) **Demographic or contact data**, such as first and last name, birth date, birthplace, ZIP code, residential street or postal address, phone number, email address, or similar public account identifiers;

(e) **Advertising identifiers**, such as Google Advertising ID, Apple ID for Advertisers, or other mobile advertising ID (MAID);

(f) **Account-authentication data**, such as account username, account password, or an answer to security questions;

(g) **Network-based identifiers**, such as **IP address** or **cookie data**; or

(h) **Call-detail data**, such as Customer Proprietary Network Information (**CPNI**).

This list emphasizes the DOJ's priorities to prevent Sensitive Personal Data or a high volume of Covered Personal Identifiers from being exploited by a Country of Concern or Covered Person. While each data field appears harmless by itself, the DSP emphasizes that once such List Identifiers are linked – or even just linkable – to another Listed Identifiers or Sensitive Personal Data, they become Covered Personal Identifiers. For example, combining an email address with an IP address, an advertising ID, or an account password could bring the dataset within the scope of the DSP. Marketing departments relying on data collection through cookies and other tracking technologies will face heightened scrutiny, far beyond what they are accustomed to.

When the volume of Covered Personal Identifiers exceeds the applicable bulk threshold of more than 100,000 U.S. persons, the DOJ Rule applies. While this threshold may seem high, the types of Listed Identifiers it covers (such as names, email addresses, IPs, and device IDs) are exchanged at scale in everyday business operations, both in B2C and B2B contexts. As a result, businesses must conduct detailed due diligence to assess whether their data collection triggers compliance obligations under the DOJ Rule.

### 2. U.S. Companies should take Proactive Steps to Mitigate Risks

Under the DSP, even business data, such as contact information found on a business card, can become a "Covered Personal Identifier" when combined with another Listed Identifier. Subject to certain limited exceptions that are fact-specific, the DSP has broad implications for everyday cross-border data analytics, cloud services, data brokerage transactions, and marketing-related data collection activities using AdTech.

To comply with the DOJ Rule, U.S. companies must proactively document their due diligence measures to mitigate enforcement risks. The DOJ guidelines emphasize that U.S. organizations cannot solely rely on the terms of contracts or assign compliance obligations to their international counterparts. Failure to conduct meaningful diligence, such as ignoring known violations or failing to validate compliance, may expose a company to enforcement actions. To comply with the DOJ Rule, US businesses should implement a risk-based data compliance program across the following critical areas:

a) **Risk Assessment and Data Mapping**:

- Identify and document all U.S. sensitive personal data and government-related data handled (by category and by volume);
- Map data flows to identify how Listed Identifiers are collected, stored, accessed, and transferred.

b) **Governance and Trainings**:

- Develop a written policy describing the data compliance program tailored to your organization's risk profile and business operations;

- Conduct training on the DSP and applicable security requirements at least annually.

c) **Due Diligence & Vendor Management**:

- Screen vendors, employees, investors, and transaction parties with ties to Covered Persons or Countries of Concern;
- Implement auditable procedures to document the types and volume of data involved and data transfer measures;
- Include contractual language prohibiting onward transfer or resale of data to Covered Persons or Countries of Concern.

d) **Security, Reporting, and Recordkeeping**:

- Ensure compliance with all technical and organizational security controls as required by the DOJ Rule;
- Report known or suspected violations to the DOJ within the mandated 14-day timelines for certain prohibited transactions;
- Maintain records of all covered data transactions, due diligence activities, compliance program documentation, and audit reports.

### 3. Key Compliance Dates and Next Steps

The DOJ Rule took effect on **April 8, 2025**. While the DOJ has stated it will not prioritize civil enforcement actions for violations occurring through July 8, 2025 – provided companies are making good faith efforts to comply – this is **not** a grace period. Businesses must act swiftly to implement necessary changes, respond to inquiries, and minimize business disruptions. As **July 8, 2025** approaches, companies should pay close attention to how they handle Listed Identifiers, which are routinely collected, stored, and transferred across everyday business transactions. With reporting requirements for certain restricted and prohibited transactions taking effect on **October 6, 2025**, this summer presents **a critical opportunity** for companies to strengthen their compliance program and ensure their data governance programs meet DOJ expectations.

For more information or assistance on this topic, please contact Vivien Peaden, AIGP, CIPP/US, CIPP/E, CIPM, PLS or a member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.