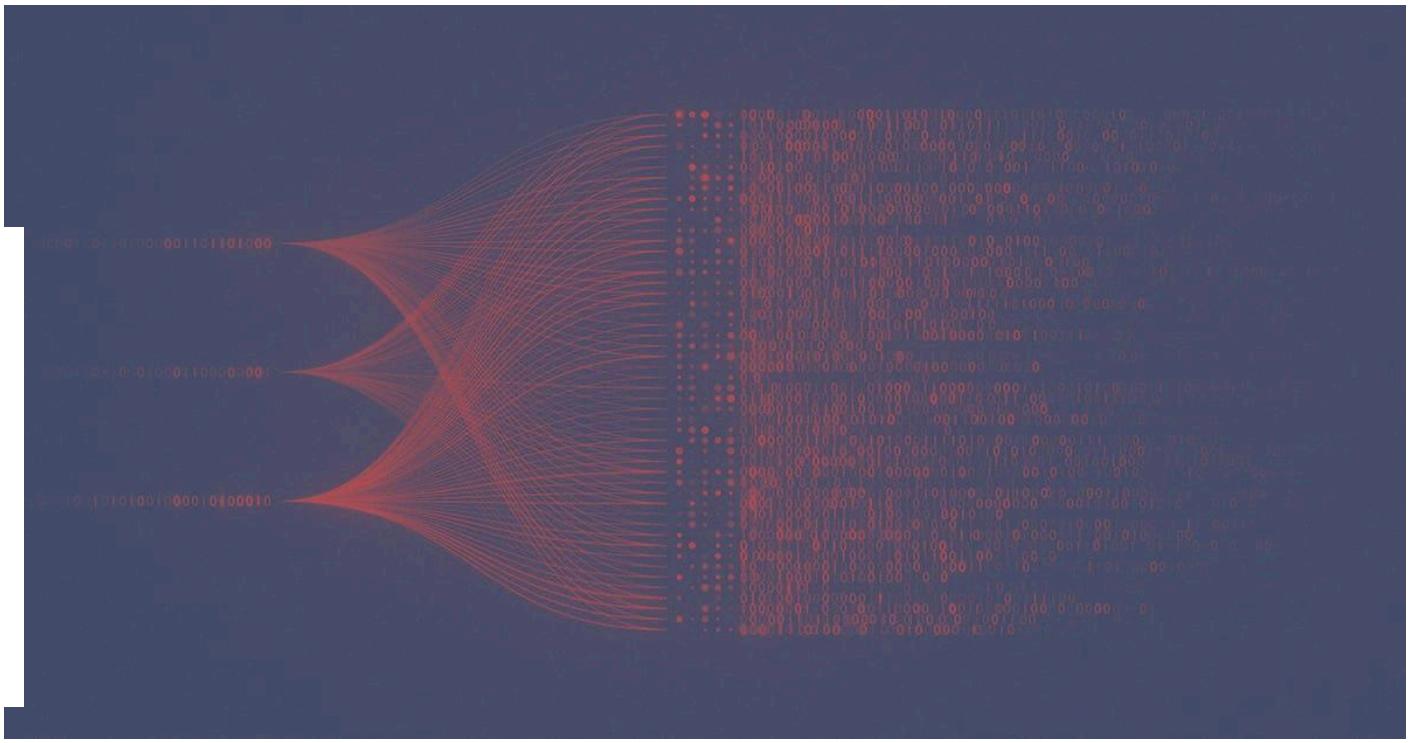
# What Compliance Leaders Need to Know Ahead of Crucial DOJ Data Security Program Deadline

Civil, criminal penalties await companies not ready to comply with new initiative

by Townsend Bourne — September 8, 2025 in Data Privacy



*The DOJ's new data security program imposes significant compliance obligations on companies handling sensitive personal or government-related data, with a critical deadline approaching in early October. Sheppard Mullin partner Townsend Bourne outlines how compliance leaders can meet national security mandates and reduce the risk of criminal and civil penalties.*

Is your business ready to comply with the full scope of the DOJ's new data security program (DSP)? If not, steep civil and even criminal penalties could be heading your way.

The new framework, which went into effect in April, imposes controls to prevent Americans' sensitive personal information and other government-related data from falling into the hands of foreign adversaries. Companies that collect and share this information in sufficient volumes are subject to the DSP's requirements — and the risk of consequential enforcement actions and fines.

Key prohibitions and restrictions on data transfers are already in place. But time is running out for companies to implement additional compliance obligations like audits, internal controls, reporting procedures and program due diligence ahead of the final Oct. 6 deadline.

# A new framework for data security

The DOJ's new program focuses on transactions involving bulk sensitive personal data or government-related data, from data brokerage and vendor agreements to employment or investment agreements. Companies are generally barred from transacting in a way that would allow individuals on the National Security Division's covered persons list or countries of concern (e.g., Russia, China, Iran, North Korea, Cuba and Venezuela) from accessing this information.

Covered data types include the genomic information, precise geolocation data and personal health or financial information of US persons, with varying volume thresholds for triggering DSP requirements. The DSP's requirements even cover transactions where the bulk data has been anonymized, aggregated or encrypted.

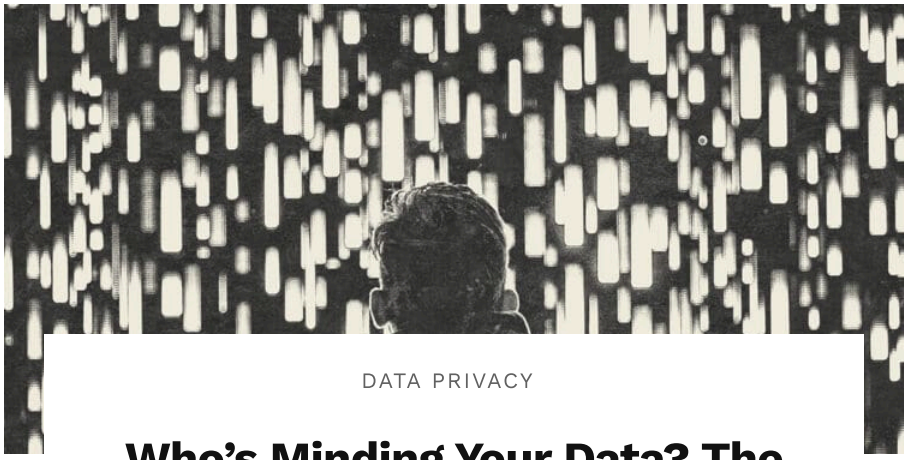
For example, the DSP covers situations where a US company hires an individual in a country of concern to help develop a new AI tool and, as a result of this employment, the individual has administrator rights to access and download bulk quantities of personal data. It also would apply to a US company that develops mobile games that collect bulk precise geolocation data and that contracts part of its software development to a covered person, allowing access to the bulk data. Other covered scenarios include appointing an individual in a country of concern to a US company's board of directors, which would allow the individual access to bulk personal financial data or engaging a foreign private equity fund located in a country of concern to provide capital for construction of a data center in the US.

While many companies have focused on the sensitive personal data requirements, it's important to remember that the DSP also regulates transfers involving precise geolocation data for any location on the government-related data list (included in the new DOJ regulations), as well as sensitive personal data marketed as linked or linkable to current or

recent former US government personnel or contractors, regardless of volume.

Additionally (and unconventionally), companies are required to make a report to the DOJ within 14 days of receiving and rejecting an offer to engage in a prohibited transaction involving data brokerage. The report should include information about the individuals requesting the transfer, the types and volume of data requested, the proposed method of transfer and accompanying documentation.

Further, as outlined in the DOJ's FAQ, there are a number of exemptions to these restrictions for specific situations, such as routine corporate group business transactions with affiliate companies overseas or certain kinds of routine financial services transfers. Still, companies that may engage in restricted transactions need to put heightened security measures in place to avoid willful violations, which could bring criminal penalties of up to $1 million in fines and two decades in prison.



DATA PRIVACY

## Who's Minding Your Data? The Case for Dedicated Privacy Leadership

by Daniel Barber JUNE 16, 2025

As state privacy laws multiply and AI introduces new vulnerabilities, the question isn't whether you need dedicated privacy expertise — it's who will fill that critical gap

# The end of the enforcement grace period

To help companies comply with the DSP's restrictions, the DOJ **offered** a 90-day grace period from the April 8 effective date, delaying action against companies making good faith compliance efforts such as:

- Assessing datasets and datatypes that might be covered by the rule.
- Reviewing data flows and data transactions.
- Analyzing vendor agreements to determine the need for new contractual terms, renegotiations and potentially new vendors.
- Instituting vendor due diligence practices.
- Evaluating employee access and potentially modifying roles, responsibilities or work locations.
- Assessing investments and investment agreements relating to countries of concern or covered persons.
- Revising or creating internal policies and procedures aligned with the DSP.
- Implementing security controls as set forth in the **requirements** established by the Cybersecurity and Infrastructure Security Agency (CISA).

That grace period ended July 8, and companies should not be surprised if the DOJ decides to make an example of those whose compliance efforts are not up to par.

# The October deadline: Programs, audits & reporting

By Oct. 6, companies covered by the DSP need to put in place numerous policies and procedures for covered data transactions, including:

**A data compliance program**, which should involve, at a minimum:

- Risk-based procedures for verifying data flows involved in any restricted transaction, including auditable methods of logging:
  - The types and volumes of data involved in the transaction.
  - The identity of the parties involved in the transaction, including any individuals' entity ownership, citizenship, or primary residence.
  - The end-use of the data.
  - The method of data transfer.
- Risk-based procedures for verifying the identity of vendors for applicable restricted transactions.
- Written policies that describe the data compliance program and the implementation of the security requirements that are annually certified by an officer, executive, or employee responsible for compliance.

**Audits**. Companies that engage in any restricted transactions will have to conduct an annual audit. The DSP framework includes specific directions for the audit's scope, timeline, and the resulting report.

**Annual reports**. Companies that engage in restricted transactions involving cloud-computing services and have 25% or more equity interests owned (directly or indirectly) by a country of concern or covered person will need to make an annual report by March 1 describing the covered data transactions during the previous year.

# Best practices for DSP compliance

With enforcement already on companies' doorsteps and new requirements coming due in October, corporate compliance leaders should ensure their programs fully align with the DSP today. The following best practices can help.

## Conduct (and document) applicability assessments

Some companies, particularly those that are not used to dealing with national security requirements, may assume that the DSP does not cover the types of data they collect or transactions they perform. However, assuming your company is out of scope is a serious mistake.

That is because the DSP's requirements go beyond transactions with covered persons and countries of concern. They also require companies to include specific contractual language for data brokerage transactions *even with foreign persons who are not covered persons under the DSP*. That means that an American company selling the health data of US persons to a company in Saudi Arabia in sufficient quantities, for example, would need to include language in the contract that prohibits the buyer from then reselling or engaging in a covered data brokerage transaction with a covered person or country or concern. Without this language, the sale becomes a prohibited transaction.

Companies should carefully assess their existing data collection practices to see whether they are amassing, storing or transacting in covered types of data in sufficient volumes to trigger DSP requirements. These assessments should be thoroughly documented in the event the DOJ later alleges that the company violated the DSP.

## Implement clear policies

Companies covered by the DSP need to have a written policy that describes their associated compliance program and is annually certified by an officer, executive or employee responsible for compliance.

A written policy alone is insufficient, however, especially with a new framework like the DSP. As with any procedural change, companies should effectively train employees on the policy, including how it will impact their day-to-day operations and any recordkeeping and reporting obligations.

## Strengthen vendor due diligence

Reviewing contract terms with vendors is an essential part of DSP compliance. Companies should carefully determine whether any of their vendors are directly or indirectly owned by covered persons or operating within countries of concern.

Using real-time screening software can help companies stay in compliance as the covered persons list is updated. The DOJ recommends that any software tools incorporate updates to the list, account for all identifiers (including alternative spellings or names), include organizational hierarchy information, consider vendors' geographical information and screen current, new and prospective vendors.

## Countdown to compliance

As the Oct. 6 deadline approaches, companies cannot afford to take a passive approach to DSP compliance. Every organization handling sensitive personal or government-related data should take steps to assess its risk, formalize compliance protocols, and prepare for regulatory scrutiny.

A proactive, well-documented compliance policy will not only help avoid enforcement but also demonstrate a serious commitment to data governance and national security.

**Tags:** Data Governance DOJ

**Previous Post**

It's Time for E&C Professionals to Have a Seat in the Boardroom

## Townsend Bourne

**Townsend Bourne** is a partner in the governmental practice in Sheppard Mullins' Washington, D.C. office. She is leader of the firm's aerospace, defense & government services team and leads the governmental practice cybersecurity & data protection team.

## Related Posts

### Administration Heightens Enforcement Focus on Tariff Evasion & 'Transshipment'


by Jessica Carey, Roberto Gonzalez, Samuel Kleiner & Samuel Rebo
SEPTEMBER 2, 2025

White House expresses zero tolerance for 'transshipment' schemes

### Dismissal of FCPA Charges Against Ex-Cognizant Execs Sends Early Sign That SEC Will Follow DOJ's Lead

by Gina Castellano, Martin Weinstein and Laura Perkins
AUGUST 13, 2025

The SEC's bribery case against a pair of former Cognizant Technology executives was six

years in the making, with pandemic·

## What You Need to Know About Healthcare Compliance and Shifting Federal Enforcement Priorities

by Noam Fischman, Ayman Rizkalla and Ameer Al-Khudari
AUGUST 12, 2025

Before-the-incident compliance is critical for healthcare cybersecurity teams

## Importers Face Increased DOJ Scrutiny & Heightened Risk for Criminal Prosecutions

by Husch Blackwell JULY 31, 2025

Criminal Division's MIMF unit expands scope to tariff fraud

# oin the conversation

*t the week's top news, opinion and events -- right to your inbox!*

ail*

ne*

ne*

untry*

Please Select

at's your current role?*

Please Select

I is committed to protecting and respecting your privacy. We will send you our weekly wsletter as requested, and from time to time, may also send you carefully screened information out webinars and downloads.

I agree. I know I can unsubscribe anytime.*

I agree to allow CCI to store and process my personal data in accordance with the privacy policy. *

Submit


LRN
From Cost Center to Catalyst:
How Ethics & Compliance Drives Business Performance
August 7 | 11 am EST
Webinar


GAN INTEGRITY
WEBINAR
Inside the Story of Tipper X
Tips for Building an Ethical Workplace
Wednesday, August 20th
10:00 AM ET / 3 PM BST
Register Today


MITRATECH
The 25 Most Important KPIs and KRIs for Third-Party Risk Management
How to Measure and Communicate TPRM Program Effectiveness to the Board
Access Now

Search...

Privacy Policy | AI Policy

*Founded in 2010, CCI is the web's premier global **independent** news source for compliance, ethics, risk and information security.*

*Got a news tip? Get in touch. Want a weekly round-up in your inbox? Sign up for free. No subscription fees, no paywalls.*

**Follow Us**

**rowse Topics:**

**CI Press**
**ompliance**
**ompliance Podcasts**
**ybersecurity**
**ata Privacy**
**Books Published By CCI**
**Ethics**
**FCPA**
**Featured**
**Financial Services**
**Fraud**
**Governance**
**GRC Vendor News**
**HR Compliance**
**Internal Audit**
**Leadership And Career**
**On Demand Webinars**
**Opinion**
**Research**
**Resource Library**
**Risk**
**Uncategorized**
**Videos**
**Webinars**
**Well-Being**
**Whitepapers**