

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

Corporate Compliance Insights

09.08.2025

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.

[Click here to read the full article.](#)

Attorneys

Townsend L. Bourne

Practice Areas

Cybersecurity & Data Protection

Governmental

National Security

Industries

Aerospace, Defense & Government Services