The DOJ's Data Security Program Rule and AdTech Risk

By Dera Nevin and Elizaveta Egorova, FTI Technology

Final affirmative obligations under the U.S. Department of Justice's Data Security Program Rule (also called the DOJ Bulk Data Transfer Rule) entered full enforcement in October 2025. The rule creates new compliance commitments for U.S. organizations that transfer or sell bulk sensitive personal data of U.S. persons internationally and restricts data flows to certain countries, entities and beneficially-owned entities listed in or identified by the Data Security Program.

The program defines "bulk sensitive personal data" to include health, biometric, genomic, financial and precise geolocation information. It also includes personal identifiers, or listed identifiers, such as IP addresses, mobile advertising IDs (e.g., GAID, IDFA), and in certain contexts can include account-authentication data (credentials, security questions) when linked or linkable to another listed identifier or to sensitive personal data. Consequently, the Data Security Program may apply to organizations that collect or process covered identifiers or other categories of sensitive personal data in bulk, if those data are made accessible to, or transferred to, a foreign country of concern and an exemption under does not apply.

Advertising technology is built on a complex ecosystem of ad platforms with global data-sharing practices and downstream data access. If those platforms or websites transmit personal data covered by the Data Security Program to servers, affiliates, or partners in or controlled by, a party or entity subject to the program, even passively, this may trigger compliance scrutiny. Transfers of persistent identifiers of U.S. persons in "bulk" quantities may qualify as a prohibited or restricted transfer depending on certain conditions. Consequently, companies that use website tracking technologies, including pixels, cookies and web beacons may need to evaluate whether they are subject to Bulk Data Rule compliance requirements.

The DOJ has emphasized the Data Security Program as an enforcement priority and violations are subject to civil or criminal penalties (potentially applicable under the International Emergency Economic Powers Act). Organizations will be expected to assess their compliance posture and evaluate whether their adtech stack vendors may be linked to entities in listed countries such as China (including Hong Kong and Macau), Cuba, Iran,

North Korea, Russia or Venezuela, or entities related to or beneficially owned by principals in those countries.

The Data Security Program lists several exemptions and exclusions to application of the rule, including:

- Personal communications
- Information or informational materials
- Travel
- Official business of the U.S. government
- Financial or telecommunication services
- Corporate group transactions
- Investment agreements subject to a Committee on Foreign Investment in the United States review
- Certain specified drug, biological product and medical device authorizations
- Clinical investigations and post-marketing surveillance data
- Specified intra-group or intra-company transfers where adequate safeguards exist
- Other transfers already regulated or approved under another federal or sector-specific regime (e.g., export controls, health care or financial services)

Outside of these exclusions, the DOJ separates covered transactions into two categories: prohibited and restricted transactions, each involving different compliance obligations and risk thresholds.

Prohibited transactions involve data brokerage activities (e.g., selling, licensing or transferring datasets) that involve government-related data or bulk U.S. sensitive personal data. The Data Security Program's definition of data-brokerage activities may encompass a wide range and is not restricted to organizations registered as data brokers under applicable state laws. It is the underlying activity involving data that counts, rather than whether a company is officially classified a data broker under U.S. laws. The Data Security Program also prohibits any transaction that gives a covered person access to bulk human "'omic" data or to human biospecimens.

Since data transfers to a country of concern or with a covered foreign person are prohibited, the Data Security Program also prohibits transactions that are structured to evade or conceal such access by a covered person, or if U.S. persons knowingly direct or facilitate others to engage in prohibited transactions. These provisions capture both direct and indirect transfers of sensitive U.S. data.

By contrast, **restricted** transactions include vendor, employment or investment agreements that could give a country of concern or a covered person access to bulk sensitive personal data or U.S. government-related data.

Restricted transactions are permitted only if all required safeguards are in place, including:

- Implemented cybersecurity controls consistent with standards issued or endorsed by Cybersecurity and Infrastructure Security Agency, such as access restrictions, localization and monitoring for systems accessed by covered persons, and specific protections for covered personal data.
- Documented, management approved and implemented Data Security Program compliance plan
- Independent audits or assessments at least on the annual basis
- Comprehensive recordkeeping requirements.

Additionally, restricted transactions require the implementation of contractual safeguards with partners or vendors receiving that data, to restrict the onward flow of covered personal data to entities covered by the Data Security Program.

When compliance risk arises

The Data Security Program covers the transfer of bulk data and defines specific thresholds for its applicability. Therefore, to evaluate risk, it is important to determine whether adtech tools collect and transmit sensitive data at scale:

- 100 individuals' genomic data
- 1,000 individuals' human epigenomic, proteomic or transcriptomic data
- 1,000 individuals' biometric identifiers
- 1,000 devices' precise geolocation data
- 10,000 individuals' health or financial data

— 100,000 individuals' covered personal identifiers (e.g., cookies, advertising IDs, IP addresses) within a year

— Combined data aggregate for the lowest number of U.S. persons or U.S. devices in that category of data

The Data Security Program makes clear that even if the datasets are labeled as de-identified, pseudonymous or encrypted, they still count toward the bulk thresholds. Large datasets containing persistent identifiers create a rich source of data. These datasets, built to maximize consumer insight and engagement, provide a potential window into U.S. consumer behavior and patterns and possibly to institutional vulnerabilities.

How organizations can evaluate adtech compliance

1. Understand website traffic metrics and telemetry. Measure the data against the thresholds established by the Data Security Program and whether tracking technologies are capturing covered data at bulk levels. Daily visitor patterns will be indicative.
2. If metrics and telemetry meet or exceed the bulk threshold, identify which categories of sensitive data they collect (health, financial, geolocation, biometric, identifiers).
3. Audit direct adtech partners. Map all direct pixel vendors, cookies, tags, analytics services and advertising partners on the websites and apps that may generate persistent identifiers or other covered data. Classify vendor risk according to location and beneficial ownership.
4. Determine if there are any prohibited transfers, including direct transfer to a country or entity covered by the DSP.
5. For data-brokerage transactions characterized as restricted transfers, involving foreign entities or persons, update contracts and data processing agreements to include DOJ-required clauses that prohibit onward transfer of covered data to any covered person, require disclosure of any such access or transfer and mandate termination if these restrictions are violated.
6. Implement technical safeguards to protect data, using routing rules, access controls and data localization. Remove or block adtech tools that cannot guarantee compliant data flows.
7. Assess whether a comprehensive and prescribed cybersecurity program and evaluation is required.
8. Establish ongoing monitoring and regularly scan digital properties to detect new or unauthorized trackers. Audit vendor disclosures against observed traffic (what can be seen firing versus what was contractually promised).
9. Maintain good recordkeeping practices, including relevant documentation, audits, compliance policies.
10. Educate and train key stakeholders involved with adtech, including privacy, legal, marketing, agencies and IT teams. All should be aware and understand the risks and compliance implications of deploying unvetted trackers on websites or apps.

The Data Security Program adds a new layer of compliance to data-driven business. For companies that rely on advertising, analytics or digital engagement, compliance will require far more than consent banners or contractual updates. Organizations are expected to have strong visibility and governance of data flows across the entire adtech ecosystem. Building those capabilities will help organizations to respond quickly as enforcement expectations evolve.

Dera Nevin
Managing Director
+1 (240) 935 3403
dera.nevin@fticonsulting.com

Elizaveta Egorova
Senior Director
+1 (202) 312 9119
elizaveta.egorova@fticonsulting.com