LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Privacy & Cyber Practice

April 23, 2025 | Number 3364

DOJ Data Security Program Now in Effect: Top Takeaways

New DOJ guidance helps companies understand their obligations under the DSP, which could severely impact investment agreements and ordinary commercial data transactions.

On April 11, 2025, the US Department of Justice (DOJ) released new guidance on its final rule, known as the "Data Security Program" (DSP), which went into effect on April 8, 2025. The DSP prevents foreign access to sensitive US data, which includes bulk sensitive personal data and government-related data ("covered data"). The guidance includes a Compliance Guide, extensive FAQs, and an Implementation and Enforcement Policy, resulting in a package of explanatory guidance materials to spur attention and compliance with the DSP.

This Client Alert provides initial enforcement considerations, top takeaways, and an Appendix summarizing the DSP.

Introduction

The DSP regulates data transactions that could grant access to US sensitive personal data to certain foreign actors with connections to "countries of concern," such as China, which the DSP refers to as "covered persons." With limited exceptions, all provisions of the DSP, including Subparts C (Prohibited Transactions, such as data brokerage) and D (Restricted Transactions, such as employment, vendor or investment agreements) went into effect on April 8, 2025. Additional affirmative and burdensome diligence, auditing, and reporting requirements from Subparts J and K will take effect on October 6, 2025, as originally announced.

The DSP and the accompanying guidance highlight the national security risks stemming from the provision of access to covered persons of bulk US sensitive personal data and government-related data. The DSP's impact will be significant in both scope and effect for US companies with a data nexus to covered persons or countries of concern. In particular, areas like foreign investments and ordinary commercial data transactions involving China and other countries of concern may now be severely limited if not totally prohibited.

The impact is magnified by the DSP's complexity. The DSP has opened a novel, rapidly evolving aspect of national security law in which navigating compliance is rarely intuitive and often diverges from commonly held policies or outcomes in data protection, export control, Committee on Foreign Investment in the United States (CFIUS), and other analogous regimes. Standing up cross-functional teams to assess whether and how the DSP rules apply and engaging in urgent "know your data" assessments should be urgent priorities.

Initial Enforcement Considerations

With the DSP in effect, companies should focus on compliance. Helpfully, DOJ's new guidance makes clear that it will not target any civil enforcement for the first 90 days, through July 8, 2025, if companies can show that they are making good-faith efforts to comply with the DSP. Instead, DOJ will focus its enforcement on criminal enforcement actions for any egregious, willful violations, including "where individuals or entities willfully violate, attempt to violate, conspire to violate, cause a violation, or engage in any action intended to evade or avoid the DSP's requirements."

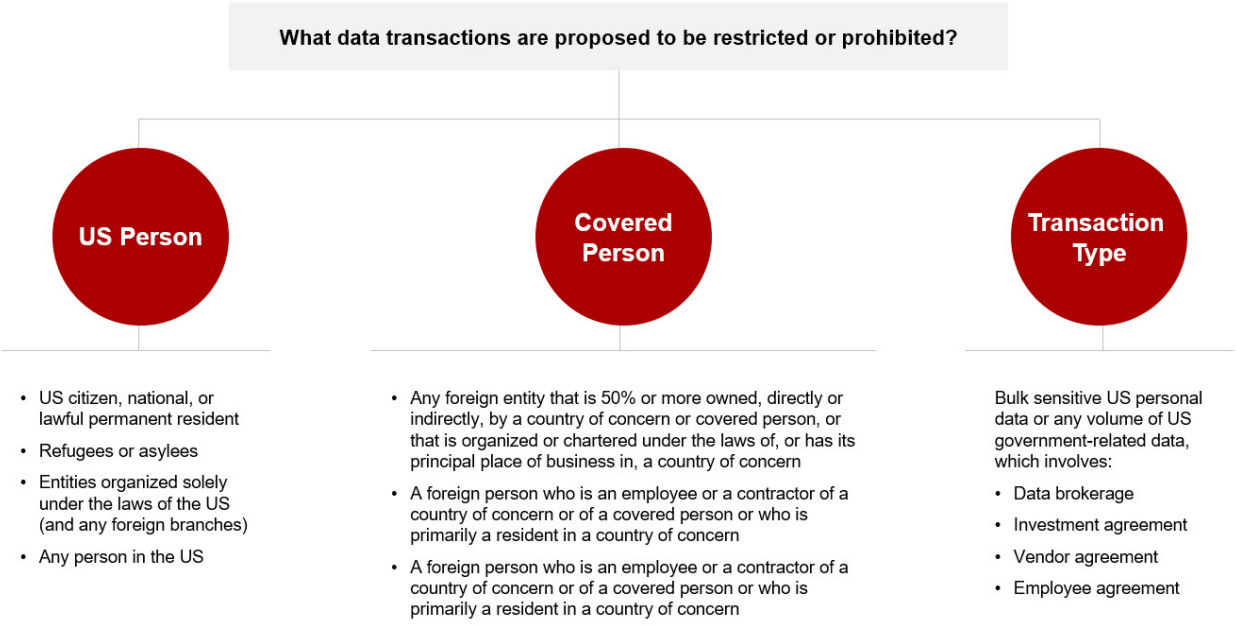
Suggested efforts to demonstrate good-faith compliance include "revising or creating new internal policies and processes, identifying data flows, changing vendors or suppliers, adjusting employee roles or responsibilities, deploying new security requirements, and revising existing contracts." DOJ expects that companies will be in *full compliance* by the end of this 90-day period.

As part of this 90-day grace period, DOJ encourages companies to reach out with informal inquiries about the DSP and highlights that it will continue to populate the FAQs periodically. This is a more informal opportunity for engagement with DOJ than under the actual DSP Advisory Opinions, which require that "the entire transaction that is the subject of the advisory opinion request must be an actual, as opposed to hypothetical, transaction and involve disclosed, as opposed to anonymous, parties to the transaction."

Top Takeaways

1. How to determine if you are transacting with a covered person

The DSP applies to the provision of access to certain US sensitive personal data by a US person to a covered person via certain covered transactions. Data flows from a US person to a US person or from a covered person to a US person do not trigger the DSP. The below graphic shows the elements of a covered data transaction under the DSP.



An individual or entity is a covered person if it meets one prong of the objective test set forth in the DSP *or* if DOJ deems the individual or entity to be under the control or influence of a covered person. Importantly, a US person is "never a covered person unless designated as such by [DOJ]" and anyone so designated will "retain their covered persons status, even when located in the United States" given DOJ's broad designation right.

If an individual or entity meets the statutory, objective test of being a covered person, the FAQs state that the individual or entity will lose its covered person status once in the United States and automatically regain their status as a covered person once outside the United States. However, given the DSP's prohibition on transactions structured to evade the DSP, companies should be particularly cautious of moving personnel around to facilitate transactions, as DOJ has stated that it will scrutinize efforts to avoid application of the DSP.

If an individual or entity is designated a covered person, it will retain this status, even when in the United States. DOJ has confirmed that it will publish the "Covered Persons List" in the Federal Register (at which point companies will be deemed to have constructive knowledge) and will also provide a version of the Covered Persons List on its website (where you can sign up for email alerts).

2. US sensitive personal data is broader than you might think

The DSP defines two sets of data as US sensitive personal data:

- Specific volumes of a listed set of categories of data (including human 'omic data, personal identifiers, health data, financial data, and more)
- Any volume of data marketed as linked or linkable to a current or former (i.e., within the two years prior to the potential covered data transaction) government employee or contractor or revealing the precise geolocation data for any location enumerated on the Government-Related Location Data List

The table below summarizes the bulk thresholds for sensitive personal data. Sensitive personal data meeting or exceeding these thresholds at any point in the preceding 12 months, whether through a single covered data transaction or aggregated across covered data transactions involving the same US person and the same foreign person or covered person, is bulk US sensitive personal data.

Bulk thresholds for US sensitive personal data

Human 'omic data about 1,000 or more individuals • Human genomic data about 100 or more individuals • Human biospecimens from which bulk human 'omic data *could* be derived
Biometric identifiers about 1,000 or more individuals
Precise geolocation data about 1,000 or more US devices
Health information about 10,000 or more individuals
Financial information about 10,000 or more individuals
Covered Personal Identifiers about 100,000 or more individuals
Any combination of the above where at least one type meets the bulk threshold

The DSP regulates covered data transactions initiated, pending, or completed on or after April 8, 2025. As such, US persons should only consider covered data transactions "in the preceding twelve months" that occur on or after April 8, 2025 (in other words, transactions before April 8, 2025, do not count toward the aggregate total).

These categories and definitions are broader and different from standard statutory or other US privacy law conceptions. DOJ has made it clear that, because "even anonymized data, when aggregated, can still be used by countries of concern and covered persons to identify individuals and to conduct malicious activities that implicate the risk to national security," minimization and obfuscation techniques common to US and international data privacy laws do not exempt the underlying data from the DSP. For example, DOJ states that even height-weight tables of Americans paired with identifiers that the recipient affirmatively cannot link back to an individual (or even IP Address) constitutes sensitive health information.

3. Investment from persons in countries of concern may be severely curtailed, unless it qualifies as "passive"

Investment in a US entity by a covered person (or country of concern) will generally trigger the DSP and the need to consider whether the transaction is restricted or prohibited when the investment does not qualify as "passive." This occurs when the covered person — whether through equity, partnership, or similar financial arrangements — obtains more than a purely capital interest, and acquires any formal or informal ability to access, influence, or participate in the US entity's decision-making or operations.

Investment agreements present unique risks because the DSP confers on covered persons "access" to bulk US sensitive personal data or government-related data in the possession of the involved US person through sufficient ownership as the result of the agreement and is agnostic to any technical (e.g., encryption of data and no key access to investors), contractual (e.g., agreements or side letters that prohibit access), or other measures designed to prevent "access." The result is that investment agreements involving covered persons may be restricted or prohibited in ways that are not intuitive and carry significant risks.

An investment agreement is an agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests or rights in relation to (1) real estate located in the United States; or (2) a US legal entity. Only narrowly defined "passive" investments are excluded. The test for a "passive" investment includes normal exclusions for public company, investment company, or similar passive investments, as well as limited partnership investments in funds or private entities. The latter types of investments will require substantial attention by deal teams, where co-investors from countries of concern are in the mix.

The DSP includes language that addresses limited partnership investments in funds or private entities. Limited partnership investments are "passive" where the investment is made as "a limited partner into a venture capital fund, private equity fund, fund of funds, or other pooled investment fund, or private entity, if the limited partner's contribution is solely capital and the limited partner cannot make managerial decisions, is not responsible for any debts beyond its investment, and does not have the formal or informal ability to influence or participate in the fund's or a US person's decision making or operations," and where it is also true that:

- the covered person has less than 10% in total voting and equity interest in a US person (could be the fund or the target/operating company); and

- the covered person does not have rights beyond those reasonably considered to be standard minority shareholder protections, including (1) membership or observer rights on, or the right to nominate an individual to a position on, the board of directors or an equivalent governing body of the US person, or (2) any other involvement, beyond the voting of shares, in substantive business decisions, management, or strategy of the US person.

The DSP includes a few fairly obvious examples of what is considered "access" in the context of investment agreements (see § 202.228). These underscore the point that unless the "passive" test above is met, all investments in US entities involving sensitive personal data will require the US company to comply with the CISA security requirements to mitigate "access" to covered data by a covered person or in a country of concern. Helpful examples from the DSP include:

- "Example 2. A foreign technology company that is subject to the jurisdiction of a country of concern and that the Attorney General has designated as a covered person enters into a shareholders' agreement with a US business that develops mobile games and social media apps, acquiring a minority equity stake in the US business. The shareholders' agreement is an investment agreement. These games and apps developed by the US business systematically collect bulk US sensitive personal data of its US users. The investment agreement explicitly gives the foreign technology company the ability to access this data and is therefore a restricted transaction." (§ 202.228(c)(2)).

- "Example 3. Same as Example 2, but the investment agreement either does not explicitly give the foreign technology company the right to access the data or explicitly forbids that access. The investment agreement nonetheless provides the foreign technology company with the sufficient ownership interests, rights or other involvement in substantive business decisions, management, or strategy such that the investment does not constitute a passive investment. Because it is not a passive investment, the ownership interest, rights or other involvement in substantive business decisions, management, or strategy gives the foreign technology company the ability to obtain logical or physical access, regardless of how the agreement formally distributes those rights. The investment agreement therefore involves access to bulk U.S. sensitive personal data. The investment agreement is a restricted transaction." (§ 202.228(c)(3)).

- "Example 4. Same as Example 3, but the US business does not maintain or have access to any government-related data or bulk US sensitive personal data (e.g., a pre-commercial company or startup company). Because the data transaction cannot involve access to any government-related data or bulk US sensitive personal data, this investment agreement does not meet the definition of a covered data transaction and is not a restricted transaction." (§ 202.228(c)(4)).

While investment agreements generally constitute restricted transactions (and may therefore be permitted, so long as they comply with the DSP's CISA requirements), there are types of investments that may now be prohibited.

For example, foreign investments in life sciences and biotechnology face distinct hurdles because the DSP both assumes an investment agreement confers "access" if the covered person acquires sufficient ownership interest and prohibits transactions involving bulk human 'omic and human biospecimen altogether (with limited exemptions). Put together, entities that possess bulk human 'omic or human biospecimens (from which bulk human 'omic data could be derived) must examine any non-passive investment from a covered person as it may be prohibited even if the investment agreement does not give the covered person actual access to the bulk data or the agreement is structured specifically to prevent the covered person from gaining access (subject to limited exemptions explained more in the Appendix).

Accepting investment from an investor in a country of concern will carry new diligence and compliance risks. And because the DSP is novel procedurally and substantively, deal teams will need input from multiple functions where cross-border investment structures are in play, whether in strategic acquisitions, across the private equity sponsor and portfolio company, or simply as a matter of operating a US business. To avoid enforcement exposure and ensure valid restricted transaction mitigation (where applicable), deal teams should establish a cross-functional working group at the outset of the investment review. This team should include:

- **Legal / compliance counsel** to interpret rule applicability, supervise CISA or CFIUS mitigation, and draft data access or other relevant clauses in investment agreements
- **Cybersecurity technical lead** to assess whether covered systems and data-level controls comply with CISA requirements, including the requirement for risk assessment
- **Privacy / data governance officer** to determine whether bulk US sensitive personal data or government-related data is held, and how it is accessed internally and externally
- **Investment operations** to evaluate contractual, governance, and information rights offered to co-investors
- **Deal sponsor / managing director** to coordinate risk appetite, materiality, and timeline for clearance, possible informal advice or license application, or mitigation steps

Unlike CFIUS, US persons comply with the DSP without active review or involvement of DOJ or other governmental authorities (unless those processes were independently required). The government does not proactively review or learn of in-scope transactions. As explained below, the DSP does allow for licensing and advisory consultations where a US person contemplating a foreign investment opportunity can engage DOJ proactively about a particular investment.

4. Data brokerage applies broadly to even first-party "commercial transactions"

Under the DSP, the term "prohibited transaction" means a data transaction involving access by a country of concern or covered person that is subject to one or more of the prohibitions described in Subpart C.

There are five categories of prohibited transactions:

i. US persons knowingly engaging in a covered data transaction involving data brokerage with a country of concern or covered person (§ 202.301)

ii. US persons knowingly engaging in a covered data transaction involving data brokerage with a foreign person (that is not a covered person) unless the US person (1) contractually requires that the foreign person refrain from onward sale with a country of concern or covered person; and (2) reports any known or suspected violations of this contractual requirement (§ 202.302)

iii. US persons knowingly engaging in a covered data transaction with a country of concern or covered person that involves access by that country of concern or covered person to bulk human 'omic data, or to human biospecimens from which bulk human 'omic data could be derived (§ 202.303)

iv. Transactions with the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in the DSP or any conspiracy formed to violate the prohibitions in the DSP (§ 202.304)

v. US persons knowingly directing any covered data transaction that would be a prohibited transaction or unauthorized restricted transaction if engaged in by a US. person (§ 202.305)

The concept of data brokerage extends beyond data brokers as they are traditionally thought of in the United States (i.e., entities that collect data about people indirectly from one source and sell it to another). The term data brokerage means the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or a vendor agreement, involving the transfer of data from any person (the provider) to any other person (the recipient), in which the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. This definition covers both first-party data brokerage (by the person that directly collected the US person's data) and third-party data brokerage (by a person that did not directly collect the US person's data, such as a subsequent reseller).

Moreover, the examples make clear that even intragroup, or common digital advertising arrangements not involving payments or sales, can constitute data brokerage. DOJ stated, when announcing the DSP, that "the phrase 'similar commercial transactions' is intended to cover other commercial arrangements (beyond just sales and licensing) involving the transfer of government-related data or bulk US sensitive personal data to countries of concern or covered persons. Commercial arrangements, by their nature, are engaged in for consideration."

Three examples in the DSP are quite telling:

- **Sharing IP Addresses and Ad IDs to Foreign Ad Exchange.** "Example 4. A US company owns and operates a mobile app for US users with available advertising space. As part of selling the advertising space, the US company provides IP addresses and advertising IDs of more than 100,000 US users' devices to an advertising exchange based in a country of concern in a 12-month period. The US company's provision of this data as part of the sale of advertising space is a covered data transaction involving data brokerage and is a prohibited transaction because IP addresses and advertising IDs are listed identifiers that satisfy the definition of bulk covered personal identifiers in this transaction." (§ 202.214(b)(4)).

- **US Ad Exchange Sharing Data to Foreign Advertisers.** "Example 5. Same as Example 4, but the US company provides the data to an advertising exchange based in the United States. As part of the sale of the advertising space, the US advertising exchange provides the data to advertisers headquartered in a country of concern. The US company's provision of the data to the US advertising exchange would not be a transaction because it is between US persons. The advertising exchange's provision of this data to the country of concern-based advertisers is data brokerage because it is a commercial transaction involving the transfer of data from the US advertising exchange to the advertisers headquartered in the country of concern, where those country-of-concern advertisers did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. Furthermore, the US advertising exchange's provision of this data to the advertisers based in the country of concern is a prohibited transaction." (§ 202.214(b)(5)).

- **Intragroup Transfers of US User Data to Parent for AI or Machine Learning Training.** "Example 6. A US information technology company operates an autonomous driving platform that collects the precise geolocation data of its cars operating in the United States. The US company sells or otherwise licenses this bulk data to its parent company headquartered in a country of concern to help develop artificial intelligence technology and machine learning capabilities. The sale or license is data brokerage and a prohibited transaction." (§ 202.214(b)(6)).

Thus, the result is that activities that are traditionally not thought of as relating to data brokerage will be captured and prohibited under the DSP.

5. Onward transfer / evasion of the DSP risks highlighted

DOJ continues to highlight the risk of onward transfer and potential intentional evasion of the DSP, referencing reminders not to structure any transactions to evade the DSP, including use of a "middleman" to ultimately provide US sensitive data to a covered person via onward transfer. In fact, despite the importance of agreements to the DSP, the only sample contractual language that was provided was with respect to the prevention of onward transfers.

Because of this focus on "middleman" transactions, it will be important for companies to honestly assess *all* transactions involving a nexus to a covered person or country of concern and ensure that they make no efforts that suggest the transaction was structured to allow it to proceed outside the scope of the DSP when it otherwise would be captured.

6. Exemptions are very narrow

The DSP allows for certain categorical exemptions in Subpart E, which include deference to the First Amendment and other federal laws and exemptions for certain financial services, intra-group transfers, drug authorizations, or clinical investigations, among others. But these exemptions are meant to be applied very narrowly, and companies should understand that they are activity-based, not entity-based.

For example, the financial services exemption will only apply to processing that is ordinarily incident to the provision of financial services, not *any* processing by a financial institution. The DSP and the accompanying guidance make clear that other processing by financial institutions, such as research and development will not be covered by these exemptions. Companies will need to look carefully at each of their transactions, including intra-group transactions, to assess whether they can truly rely on any of the categorical exemptions.

7. It is critical to "know your data"

The guidance repeats the same theme throughout: companies need to know their data: "Specifically, U.S. persons should have awareness of the type and volume of their data and whether they maintain or deal in government-related data and bulk U.S. sensitive personal data." As above, providing access (to a covered person) to covered data via data brokerage or a vendor, employment, or investment agreement will trigger compliance requirements with the DSP, so it is important to understand how the data flows in and out of your company.

Companies need to understand:

- The kinds and volumes of data collected about or maintained on US persons or US devices
- How the data is used
- Whether the company engages in covered data transactions
- How such data is marketed, particularly with respect to current and former government employees and contractors (i.e., emphasis on government-related data)

Importantly, US persons are not required to de-aggregate or decrypt their information to fully assess whether they are processing US sensitive personal data. Instead, the FAQs suggest that companies rely on other metrics, such as user statistics, to "estimate the number of impacted individuals for the purposes of identifying whether a particular transaction meets the bulk threshold" and references the fact that many companies are already engaged in a similar exercise under data breach notification laws.

Knowing your data will also help companies to prepare for any future designations by DOJ on the Covered Persons List. If you have a decent understanding of your data flows and various controls over that data, you should be able to pivot in a relatively frictionless fashion.

8. Long lead time may be needed for compliance with due diligence and vendor management requirements by October 2025

A large part of the guidance is devoted to the "Data Compliance Program" that companies should stand up to assist with compliance with the DSP. An important part of the Data Compliance Program will be conducting and documenting due diligence of third parties with which companies will be transacting (in addition to the "know your data" requirements discussed above).

Companies engaging in vendor agreements with foreign person entities "will not be expected, as part of their Data Compliance Program, to conduct due diligence on the employment practices of the foreign person entity to determine whether the foreign person entity's employees qualify as covered persons" or determine "the extent to which an entity or individual is subject to the influence or control of a country of concern or covered person." However, the FAQs make clear that this does not eradicate the responsibility to conduct due diligence, stating that US persons have the "obligation to take reasonable steps, as part of a risk-based compliance program, to ascertain whether ... individuals and entities fall into one or more of [the] categories of covered persons."

Importantly, while the Data Compliance Program obligations do not come into effect until October 6, 2025, certain components will be helpful in showing good-faith compliance with the requirements around prohibited and restricted transactions that are now in effect. For example, DOJ has suggested that good-faith efforts to comply could include the following:

- Identifying data flows
- Changing vendors or suppliers
- Revising existing contracts

The table on the next page shows suggested "know your data" and "good faith" compliance efforts.

Suggested "know your data" and "good faith" compliance efforts

Conducting internal reviews of access to sensitive personal data, including whether transactions involving access to such data flows constitute data brokerage
Reviewing internal datasets and datatypes to determine if they are potentially subject to DSP
Renegotiating vendor agreements or negotiating contracts with new vendors
Transferring products and services to new vendors
Conducting due diligence on potential new vendors
Negotiating contractual onward transfer provisions with foreign persons who are the counterparties to data brokerage transactions
Adjusting employee work locations, roles, or responsibilities
Evaluating investments from countries of concern or covered persons
Implementing the CISA requirements, including the data-level requirements

9. Deploy role-based training for all relevant personnel

The Data Compliance Program should be tailored based on the company's risk profile but should be sure to include written policies and procedures (including a written security policy that demonstrates implementation of the CISA requirements). Failure to maintain documented policies and procedures can be considered "an aggravating factor in any enforcement action." Companies should also ensure that all relevant employees are kept up to date and trained on the details of the DSP (such as the company's Data Compliance Program policies and procedures), including by assessing their knowledge via training assessments.

In addition to general personnel training, companies should prepare to hire, or designate internally, a senior employee with technical expertise to lead the Data Compliance Program and be prepared to allocate resources to support the Data Compliance Program. This compliance manager should also be prepared to sign an annual certification (sample language has been provided in the guidance).

Importantly, this effort is going to require companies to lean on subject matter expertise across the business, including privacy, sanctions, and export controls. This varied expertise will be useful in quickly understanding and complying with the DSP, which, as highlighted in both the DOJ discussion around the DSP and the FAQs, has been created out of an inter-agency effort (see, for example, FAQs 8, 9, 10, and 48 in which DOJ discusses how the DSP should be read in connection with rules from other agencies, such as the Office of Foreign Assets Control).

10. Assess your reporting and auditing requirements

Companies should conduct periodic risk assessments (at least annually, and in the case of certain events, such as investments or other corporate transactions or apparent violations of the DSP). This risk assessment will inform the continued development and maintenance of the Data Compliance Program.

DOJ suggests that the assessment could include a review of the following:

- Current security measures
- Vendors, investors, and employees
- Offered products and services
- Coverage under existing licenses or exemptions
- The geographic locations of the organization and its vendors, subsidiaries, parent organizations, intermediaries, and counterparties

Companies should also audit their Data Compliance Program annually using an independent auditor (who may be an internal stakeholder so long as there is sufficient independence). The audit should be designed to detect compliance gaps with security requirements, compliance program policies and procedures, as well as all related software and technology. While other third-party audit processes may be used to satisfy this audit requirement (e.g., NIST, SOC) it is important to ensure that all the unique requirements and aspects of the DSP are accounted for.

Finally, any company that engages in a restricted transaction involving cloud computing services, and that meets certain other requirements, is required to file an annual report unless otherwise prohibited by law.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Heather B. Deixler
heather.deixler@lw.com
+1.415.395.8110
San Francisco

Clayton Northouse
clayton.northouse@lw.com
+1.202.637.3371
Washington, D.C.

Michael H. Rubin
michael.rubin@lw.com
+1.415.395.8154
San Francisco

Max G. Mazzelli
max.mazzelli@lw.com
+1.415.395.8040
San Francisco

Brianna Gordon
brianna.gordon@lw.com
+1.202.521.5745
Washington, D.C.

Kiara E. Vaughn
kiara.vaughn@lw.com
+1.617.880.4658
Boston

Appendix: Summary of the DSP's Requirements

The DSP places significant obligations on US persons, who must manage enforcement risks and compliance requirements if they permit access to covered data (bulk US sensitive personal data or government-related data by entities or employees in any of the six designated countries of concern. Compliance is particularly crucial for US companies engaged in cross-border data transfers, especially those dealing with large volumes of sensitive or government-related data. Non-compliance with the DSP can lead to civil penalties of up to $368,136, criminal fines up to $1 million, and imprisonment for up to 20 years.

Applicability of the DSP

To be subject to the DSP, a transaction must involve specific elements such as US persons, covered persons, covered data, and specified data transactions.

US Person: The DSP imposes restrictions and obligations on US persons, defined as:

- US citizens, nationals, or lawful permanent residents
- Individuals admitted to the US as refugees or granted asylum
- Entities organized under US laws or any jurisdiction within the US, including foreign branches
- Individuals or entities physically present in the US

Notably, a US company that is a subsidiary of a foreign company, such as one headquartered in China, is considered a US person, not a covered person unless otherwise designated as such.

Covered Person: Transactions are covered if they involve a US person providing access to a covered person, which includes:

- Foreign entities 50% or more owned by a country of concern, organized under its laws, or with their principal place of business there
- Foreign entities 50% or more owned by a covered person
- Foreign employees or contractors of countries of concern or entities that are covered persons
- Foreign individuals primarily residing in countries of concern

Any person or entity designated by DOJ, regardless of location, if determined to be controlled by or under the jurisdiction of a country of concern or covered person

Countries of Concern: The DSP designates six countries — China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela — as countries of concern due to their adverse conduct toward US national security. This list can change based on determinations by the Attorney General, Secretary of State, and Secretary of Commerce.

Covered Data: The DSP regulates transactions involving access to:

- **Sensitive Personal Data:** Specific volumes of data in six categories:
  - Human genomic data about 100 or more individuals (e.g., data representing nucleic acid sequences that comprise the entire set or a subset of the genetic instructions found in a human cell, including results of a "genetic test" and biospecimens)
  - Human epigenomic, proteomic, or transcriptomic data about 1,000 or more individuals (e.g., results from an individual's genetic test, DNA methylation, histone modifications, or systems-level analysis of RNA transcripts and proteins expressed by human genomes)
  - Biometric identifiers about 1,000 or more individuals (e.g., facial images, voice prints/patterns, retina/iris scans, palm/fingerprints, gait, keyboard usage pattern that are enrolled in a biometric system)
  - Precise geolocation data about 1,000 or more US devices (e.g., data, whether real-time or historical, that identifies location of device/individual)
  - Health information about 10,000 or more individuals (e.g., height, weight, vital signs, symptoms, test results, diagnosis, diagnostics, and digital dental records)
  - Financial information about 10,000 or more individuals (e.g., data about an individual's credit, charge or debit card, or bank account (including purchase/payment history); data in bank/credit statement; "consumer reports")
  - Covered personal identifiers about 100,000 or more individuals (identifiers would include those reasonably (and commonly) linked to an individual such as government ID, Social Security number, full financial account number, MAC / IMEI or other device identifiers)
  - Any combination of the above in which at least one type meets the bulk threshold
- **Government-Related Data:** Any volume of data that could reveal insights about US government locations or personnel, including precise geolocation data for areas designated by the Attorney General, such as military installations or intelligence facilities, and sensitive personal data linked to US government employees or officials.

Prohibited or Restricted Covered Data Transactions Under the DSP

The DSP has indicated the types of transactions that will be (1) prohibited wholesale, (2) restricted if certain security requirements and other obligations are met, or (3) fully exempted from the scope of the DSP.

- **Prohibited Transactions**
  - US persons knowingly engaging in a covered data transaction involving data brokerage with a country of concern or covered person (§ 202.301)
  - US persons knowingly engaging in a covered data transaction involving data brokerage with a foreign person (that is not a covered person) unless the US person (1) contractually requires that the foreign person refrain from onward sale with a country of concern or covered

person; and (2) reports any known or suspected violations of this contractual requirement (§ 202.302)

- US persons knowingly engaging in a covered data transaction with a country of concern or covered person that involves access by that country of concern or covered person to bulk human 'omic data, or to human biospecimens from which bulk human 'omic data could be derived (§ 202.303)

- Transactions with the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in the DSP or any conspiracy formed to violate the prohibitions in the DSP (§ 202.304)

- US persons knowingly directing any covered data transaction that would be a prohibited transaction or unauthorized restricted transaction if engaged in by a US person (§ 202.305)

- **Restricted Transfers:** The DSP imposes security restrictions (as published by CISA) on:

  - *Vendor agreements*: any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration.

  - *Employment agreements*: any agreement or arrangement in which an individual, other than an independent contractor, performs work or job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level.

  - *Certain investment agreements*: any agreement in which a person, in exchange for payment or other consideration, acquires direct or indirect ownership interests or rights related to real estate located in the United States or a US legal entity.

Starting October 6, 2025, US persons involved in restricted transactions must establish compliance programs, conduct audits, and maintain records. Reporting requirements will also be enforced for particular transactions, including those involving cloud-computing services or rejected prohibited transactions.

The DSP provides exemptions for prohibited or restricted transactions in certain narrowly drafted scenarios. Exempt transactions include:

- **Personal communications:** transactions involving personal communications that do not transfer "anything of value"

- **Information or informational materials:** transfers of commercial or non-commercial information, such as published materials or publicly available research

- **Travel:** transactions that are ordinarily incident to travel to or from any country, including importation of accompanied baggage for personal use; maintenance within any country, including payment of living expenses and acquisition of goods or services for personal use; and arrangement or facilitation of such travel, including non-scheduled air, sea, or land voyages

- **Official business of the US government:** transactions that relate to the conduct of the official business of the US government by its employees, grantees, or contractors; any authorized

activity of any US government department or agency or transactions conducted pursuant to a grant, contract, or other agreement entered into with the US government.

- **Financial services:** transactions ordinarily incident to and part of providing financial services, such as banking, capital markets, futures or derivatives, or financial insurance services; financial activities authorized for national banks; activities defined as financial in nature or complementary to a financial activity; transfer of personal financial data incidental to e-commerce; and the provision of investment management services that provide advice on portfolios or assets for compensation, including related ancillary services.

- **Corporate group transactions:** transactions between a US person and its subsidiary or affiliate located in or directed by a country of concern if they are "ordinarily incident to and part of administrative or ancillary business operations," such as human resources, payroll, taxes, permits, compliance, risk management, travel, and customer support.

- **Transactions required or authorized by US federal law or international agreements, or necessary for compliance with federal law**

- **Investment agreements subject to CFIUS action**

- **Telecommunications services:** transactions, other than those involving data brokerage, that are ordinarily incident to and part of the provision of telecommunications services

- **Drug, biological product, and medical authorizations:** data transactions including "regulatory approval data" necessary to obtain or maintain regulatory approval

- **Other clinical investigations and post-marketing surveillance data:** transactions that are part of clinical investigations regulated by the Food and Drug Administration (FDA), or that support FDA applications for research or marketing permits for drugs, biological products, devices, combination products, or infant formula, and include de-identified or pseudonymized data in accordance with FDA regulations.

Reporting and Auditing Requirements

Recordkeeping (10-Year Retention Requirement): All US persons engaging in covered transactions must retain complete and accurate records for at least 10 years. Additional documentation is required for restricted transactions, including the following:

- Written and annually certified data compliance and cybersecurity policies

- Annual security audits and certifications

- Due diligence documentation (including data types, volume, transfer methods, parties' identities, and end-use)

- Agreements, licenses, and DOJ-issued references related to the transaction

- Annual certification affirming the completeness and accuracy of due diligence records

On-Demand Reporting: DOJ may require reports at any time — before, during, or after a transaction — regarding any act, transaction, or data exchange covered under this rule. This includes:

- Full disclosure of books, contracts, emails, metadata, text messages, and other records
- Production in a usable format in accordance with DOJ data delivery standards

Annual Reports: US persons engaged in restricted cloud-computing transactions — in which 25% or more ownership is held by a country of concern or covered person — must file annual reports that include:

- Transaction details (data types, volume, methods of transfer, and parties involved)
- Documentation of the transaction and foreign involvement
- Contact information for responsible compliance personnel

Reporting Rejected Transactions (Within 14 Days): US persons who affirmatively reject a prohibited data brokerage transaction must report (including any rejections via automated software):

- Description of the rejected transaction and involved parties
- Documentation created or received in relation to the rejected offer

Licensing

- **General Licenses:** DOJ may issue general licenses that authorize a category of otherwise restricted or prohibited transactions. They will be published on the DOJ website and include:
  - The types of data and transactions authorized
  - Eligible counterparties or jurisdictions
  - Any applicable conditions, limitations, or ongoing obligations

General licenses do not retroactively authorize prior transactions.

- **Specific Licenses:** US persons may also apply for a specific license to engage in a particular prohibited or restricted transaction. Applications must include:
  - Identity of all parties to the transaction (including foreign affiliates)
  - Nature, volume, and sensitivity of data involved
  - Geographic location of access or processing
  - Mitigation measures implemented or planned
  - DOJ aims to respond within 45 days, though timelines are not binding

A specific license, once issued, may impose affirmative conditions and compliance obligations tailored to the transaction.

Advisory Opinions

- DOJ will issue advisory opinions to clarify whether a proposed transaction would be subject to the rule.
  - Must relate to a concrete and prospective transaction; hypothetical scenarios will not be considered
  - Requests must describe:
    - Parties involved
    - Data types at issue
    - Proposed controls or safeguards
- DOJ intends to issue opinions within 30 days, subject to extension if needed.

Emerging Obligations Vary by Industry and Maturity Level

While the DSP applies broadly to US persons engaging in covered data transactions, its practical impact varies significantly based on the sector, data sensitivity, and corporate structure. Find more industry-specific guidance in this blog post.