Steptoe

# **Steptoe White Paper:** The DOJ's New Data Security Program

OCTOBER 2025

*This white paper was originally published in May 2025 and has been updated to reflect recent developments as of October 2025.*

# Executive Summary

The US Department of Justice (DOJ) recently began enforcement of sweeping new rules regarding the transfer and storage of sensitive US data in July 2025. The rules prohibit transfers of sensitive personal data and US government-related data to certain countries of concern and persons affiliated with those countries, either directly or indirectly. Violations of the rules can result in significant civil or criminal penalties for individuals and companies. The new rules also mandate certain due diligence and auditing requirements, as well as contractual language when engaging in data transactions with any foreign party. This white paper, authored by members of our National Security, Data Privacy, and White-Collar practices, provides a detailed analysis of the newly enacted regulations, including the types of transactions they prohibit or restrict, and outlines the necessary actions that corporations and individuals must take to ensure compliance with these rules.

# I. Introduction

In January 2025, the US Department of Justice (DOJ) finalized a sweeping set of new regulations regarding the protection of "bulk sensitive personal data" and US government-related data. The program, known as the Data Security Program (DSP), imposes stringent requirements designed to prevent such data from flowing to "countries of concern" and certain persons affiliated with those countries, with potentially significant criminal and civil penalties for violations. The DSP applies not only to data brokerage or similar transactions, but also to the transfer of data associated with vendor, employment, and investment agreements, potentially having a broad impact across multiple aspects of a company's operations. The rules became effective on April 8, 2025, although DOJ provided a 90-day grace period for enforcement against most violations.

While initiated under former President Biden's Executive Order (EO) 14117, the Trump administration is fully implementing and enforcing the rules. The DOJ's National Security Division (NSD) promulgated the final rule implementing EO 14117, codified at 28 CFR Part 202, on January 8, 2025. On April 11, NSD issued a Compliance Guide, a list of over 100 Frequently Asked Questions (FAQs), and an Implementation and Enforcement Policy for the first 90 days. While NSD has long played an important role in prosecuting criminal violations of national security-related laws, it has not historically acted as a regulator in the area of technology or data transfers, as it now will under the DSP.

Based on both public statements and conversations with individuals familiar with the DOJ's plans, we expect that the Trump administration will emphasize enforcement efforts surrounding the Data Security Program. Indeed, in the DOJ's April 8 announcement, Deputy Attorney General Todd Blanche made the DOJ's policy goals clear, stating, "If you're a foreign adversary, why would you go through the trouble of complicated cyber intrusions and theft to get Americans' data when you can just buy it on the open market or force a company under your jurisdiction to give you access? … The Data Security Program makes getting that data a lot harder."

The NSD began enforcement in July 2025. NSD has strongly encouraged individuals and

companies who might be impacted by the new enforcement regime to review the DSP rules and implement new compliance policies and procedures. Which sectors are most impacted will become clearer over time, but companies in the artificial intelligence, financial services, data brokerage, information technology, healthcare, life sciences, and consumer sectors are likely to face increased exposure due to the nature of their business operations and the sensitivity of their acquired and stored data. Businesses with significant cross-border activities will likely be most impacted by the DSP rules. However, businesses with a primarily domestic presence may still be subject to the DSP given its significant breadth and impact on vendors, employees, and investors, in addition to data brokerage.

The DSP rules mirror, to some degree, requirements applicable in other jurisdictions, such as European Union (EU) Data Protection requirements, which impose restrictions on the transfer of personal data outside of the EU. These rules are also aligned with the current concerns and scrutiny of EU Data Protection Authorities regarding the transfer of personal data to China. In light of these developments and given the DOJ's stated priority concerning data protection going forward, companies should carefully consider how to navigate and comply with the new rules and the rapidly changing enforcement climate. In particular, global companies may need to consider how the DSP rules intersect with their obligations under other regimes and revise existing data security and privacy policies and procedures targeted at compliance with those non-US laws. Steptoe stands ready to provide guidance and address any questions you may have regarding the new data protection regulatory regime.

The following memorandum explains: 1) what the Data Security Program entails and the compliance requirements for US and foreign companies; 2) the necessary actions companies should take to comply with the requirements; and 3) how Steptoe can support and advise clients in effectively implementing these changes.

To begin, we list the key questions that companies and individuals should be asking regarding their current or future data transactions:

**Critical Questions to Consider Under the DSP**

1. Evaluate whether the company or individual is a *US Person*.
2. Is the data recipient a *Country of Concern* or a *Covered Person*?
3. Is the transaction a *Covered Data* Transaction?
4. What is the nature of the data being transferred?
    a) Does it involve "Bulk" US sensitive personal data?
        i) If so, does it meet personal data thresholds?
    b) Does it involve "Government-related data"?
5. What is the arrangement under which the data is being transferred?
    a) Data brokerage agreement?
    b) Vendor agreement?
    c) Employment agreement?
    d) Investment agreement?
6. Does the transfer provide *Country of Concern* or *Covered Person* access to the data in question?
7. Can the transfer be conducted as a Restricted Transaction?
8. Is there any other exemption that permits the transfer to proceed?

# II. Prohibited and Restricted Transactions

The DSP is complex, and the full scope of its reach will remain uncertain until NSD clarifies its enforcement priorities. In the following section, we provide an explanation of the structure and application of the new regulatory regime.

At its base, the DSP prohibits US Persons from engaging in certain types of transactions, many of which might be common data transactions for certain companies or in other instances may only be tangentially related to data. In certain cases, transactions are considered "restricted," as opposed to "prohibited," meaning US Persons may engage in such transactions provided they adhere to a variety of requirements including creation of a compliance program and implementation of various data security measures. We discuss the criteria for these transactions in detail below. In order to understand those criteria, it is important to define three key terms in the regulations: "Country of Concern," "Covered Person," and "U.S. Person." We turn to the definitions of these terms first before analyzing their application under the DSP.

## A. Key Regulatory Terms

### 1. Country of Concern

The Attorney General determined, with the concurrence of the Secretaries of State and Commerce, that the following countries are "Countries of Concern" as listed in § 202.601:

- China (including Hong Kong and Macau)
- Cuba
- Iran
- North Korea
- Russia
- Venezuela

The Final Rule explained NSD's view that the governments of these countries "have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of U.S. persons, and pose a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or the security and safety of U.S. persons." Notably, Section 2(f) of EO 14117 authorizes the Attorney General to identify new or remove existing countries of concern going forward.

### 2. Covered Persons

Executive Order 14117 directed the DOJ to identify classes of "Covered Persons." Notably, "Person" means an individual or entity under the regulations, and a "Foreign Person" means any person that is not a US Person (defined below). The categories of Covered Persons as set forth in § 202.211(a) are described on the following page. Importantly, a Covered Person includes not just entities and individuals physically located in a Country of Concern but also includes several additional categories of persons with less direct relationships to Countries of Concern.

### Category 1 – Certain Foreign Companies

- Foreign entity that is at least 50% owned (directly, indirectly, or in the aggregate) by one or more Countries of Concern or a Category 2 entity;

  OR

- Foreign entity organized or chartered under the laws of a Country of Concern;

  OR

- Foreign entity that has its principal place of business in a Country of Concern.

***Example**: Acme Corp. is a Cayman Islands registered corporation with its headquarters in Shenzhen, China. Acme Corp. is a Covered Person as it is a foreign person located in China, a Country of Concern.*

### Category 2 – Certain Foreign Companies

- Foreign entity that is at least 50% owned (directly, indirectly, or in the aggregate) by one or more Category 1, 3, 4, or 5 persons.

***Example**: Through its various subsidiaries, Acme Corp. is a 51% owner of a joint venture, Acme France, which is registered in France and headquartered in Paris. Acme France is a Covered Person because it is a Foreign Person that is at least 50% owned by a Category 1 person.*

### Category 3 – Certain Employees & Contractors

- Foreign individual who is an employee or contractor of a Country of Concern or of a Category 1, 2, or 5 entity.

***Example**: Employee A is a South Korean national residing in Seoul who is working as a contractor for Acme France on the development of Acme France's customer payment platform. Employee A is a Covered Person because she is a contractor of a Category 2 entity.*

### Category 4 – Certain Individuals

- Foreign individual who is primarily a resident in the territorial jurisdiction of a Country of Concern.

***Example**: Person B is a Swiss national who resides in Moscow, Russia. Person B is a Covered Person because of his residence in Russia, a Country of Concern.*

### Category 5 – Persons Determined by the Attorney General

- Any Person, wherever located, determined by the Attorney General:

  (i) To be, to have been, or to be likely to become owned or controlled by or subject to the jurisdiction or direction of a Country of Concern or Covered Person;

  (ii) To act, to have acted or purported to act, or to be likely to act for or on behalf of a Country of Concern or Covered Person; or

  (iii) To have knowingly caused or directed, or to be likely to knowingly cause or direct a violation of this part.

***Example 1**: Person C is a US national working in Singapore who provided strategic business advice to Acme Corp. on its acquisition of bulk sensitive data. The Attorney General determines that Person C is a Covered Person for acting or being likely to act on behalf of Acme Corp., a Covered Person.*

***Example 2**: Company Z is a Delaware registered, New York headquartered software development firm. Acme Corp. acquires a majority ownership in Company Z. The Attorney General determines that Company Z is a Covered Person because it is owned or controlled by Acme Corp., a Covered Person.*

The regulations also provide examples of persons who are not Covered Persons, including but not limited to:

- A citizen of a Country of Concern (e.g., a Chinese citizen) that is located in the US. This person would be treated as a US Person and not a Covered Person, except to the extent the person is individually designated as a Covered Person by the DOJ.
- A citizen of a Country of Concern (e.g., a Russian citizen) that is located in a third country that is not a Country of Concern (e.g., the UK). This person would not be a Covered Person unless the person was (i) individually designated by the DOJ or (ii) an employee or contractor of the government of a Country of Concern or a Covered Person entity.
- An entity incorporated in the US that is 50% or more owned by a Covered Person, unless the entity is individually designated as a Covered Person by the DOJ.

Given the significant breadth of the definition of Covered Person, it is important for companies to conduct careful due diligence on their vendors, employees, investors, and other persons to whom they make covered data available. We note that category five of Covered Persons potentially applies to *all* persons, regardless of citizenship or location, meaning even a US citizen or US incorporated entity can be a Covered Person if the Attorney General determines that the individual/entity meets one of the criteria listed in category five. Examples of individuals and entities that would meet the criteria for a determination by the Attorney General include:

- A US subsidiary owned or controlled by a Chinese-headquartered company.
- A US company that the Attorney General determines "to be likely to become" owned or controlled by a Russian-headquartered company.
- A US employee, contractor, or vendor acting for or on behalf of a Chinese-headquartered employer.

Notably, although these US Persons meet the criteria for a determination, the Attorney General has discretion on whether to designate an individual or company as a Covered Person. At this early stage and before DOJ has established a clear enforcement pattern, it is unclear how DOJ will use its discretion under the regulations. The DOJ announced that it will in the future publish an initial Covered Persons List, which will identify the individuals and entities that DOJ has determined to be Covered Persons pursuant to its discretionary authority. We expect that this initial list of Covered Persons will aid in better understanding the DOJ's priorities with respect to the determinations of Covered Persons. At this early stage, we encourage impacted persons to consult with counsel if questions arise as to whether or not a transaction partner meets the definition of a Covered Person.

We note also that the DSP includes a path to challenge a Covered Person designation and seek removal from the list. It appears that, among other considerations, DOJ may grant removal on the basis of remedial steps taken by the applicant. Section 202.702 indicates that the removal process may be similar to the delisting processes used in other national security contexts (e.g., for parties seeking removal from a US economic sanctions or export controls list). However, the details are limited at this time and NSD has stated that it

will release more information regarding the removal process in the future.

### 3. US Persons

The DSP rules apply to "U.S. Persons," including US citizens, nationals, lawful permanent residents, refugees, and asylees, as well as entities organized solely under the laws of the United States (including foreign branches of US companies), and any persons within the United States. Some examples of Foreign Persons and US Persons include:

- An individual citizen of a Country of Concern located in the United States is a US Person.
- A dual citizen of the US and a Country of Concern is a US Person, regardless of location.
- If a company is organized under the laws of the United States and has a foreign branch in a Country of Concern, the company, including its foreign branch, is a US Person. Likewise, if a company is organized under the laws of a Country of Concern and has a branch in the US, the company, including its US branch, is a Foreign Person.
- In contrast to branches, subsidiaries are treated separately from their parent companies with respect to US Person and Foreign Person determinations. In other words, if a parent company organized under the laws of the United States has a subsidiary organized under the laws of a Country of Concern, the parent is a US Person and the subsidiary is a Foreign Person, regardless of the degree of ownership by the parent company. However, it is important to remember that Foreign Person entities can be Covered Persons by virtue of their ownership structure, as described above.

## B. Transaction Criteria

Next, we turn to a discussion of the necessary criteria that a transaction must meet in order to be subject to the DSP. For a data transaction by a US Person to fall under the DSP's purview, it must meet the following three criteria:

1. The transaction must be a "Covered Data Transaction";
2. The "Covered Data Transaction" must involve either:
   a) "Bulk" US sensitive personal data, or
   b) "Government-related Data"; and
3. The transaction must involve providing a "Country of Concern" or a "Covered Person" with "Access" to the data at issue.

We discuss each of these criteria in more detail below.

### 1. What is a Covered Data Transaction?

Under § 202.210(a), a "Covered Data Transaction" is a transaction that involves any access by a Country of Concern or a Covered Person to any 1) government-related data or 2) bulk US sensitive personal data and that involves one of the following types of arrangements: a) data brokerage; b) a vendor agreement; c) an employment agreement; or d) an investment agreement.

- The term "data brokerage" is defined in the rules at § 202.214(a) as "the sale of data, licensing or access to data, or similar commercial transaction … involving the

transfer of data from any person to any other person, where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data."

- A "vendor agreement" is defined in the rules at § 202.258(a) as "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."

- An "employment agreement" is defined in the rules at § 202.217(2) as "any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs 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."

- An "investment agreement" is defined in the rules at § 202.228(a) as "an agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to: (1) Real estate located in the United States; or (2) A U.S. legal entity." The definition contains an exclusion for certain "passive investments" meeting criteria enumerated in the regulations.

The DSP rules contain examples of transactions that do and do not fall within each of the above enumerated categories. Entities and individuals are encouraged to carefully consider whether their data transactions fall within one of the above categories.

## 2. Covered Data

The Data Security Program rules only apply to the transfer of and access to certain types of data (collectively referred to as "Covered Data"). We discuss these types of data in detail below. Companies and individuals should consult with counsel to analyze whether or not their data fits within one of the categories of data at issue in the Data Security Program. In addition, companies should remain mindful that new lines of business or new acquisitions may trigger obligations under the Data Security Program. Companies should also be aware that the Attorney General has the authority to promulgate further regulations pursuant to EO 14117, meaning other categories of data may get added to the scope of the DSP.

### a. Government-Related Data

As defined at § 202.222, two types of government-related data currently fall under the DSP. The first includes any "precise geolocation data," regardless of volume, for any location within any area enumerated on

the Government-Related Location Data List contained at § 202.1401. The second type of government-related data includes any sensitive personal data marketed as linked or linkable to current or recent former employees, contractors, or officials of the US government, including but not limited to the military and the intelligence community, regardless of volume.

b. Bulk US Sensitive Personal Data

The DSP also regulates certain transactions involving "Bulk U.S. Sensitive Personal Data." Under § 202.206, this data means "a collection or set of sensitive personal data relating to U.S. Persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted, where such data meets or exceeds" certain bulk thresholds as set forth in § 202.205 and in the table below. Sensitive personal data involves data falling within several enumerated categories, including: geolocation data, biometric identifiers, human 'omic data, personal health data, financial data, or any combination thereof. Each category of sensitive personal data is defined in detail within the regulations. Companies that believe they may have data touching on these categories should carefully review those definitions to determine if a given category applies.

The regulations specify bulk data thresholds for each of these categories. The volume of data is measured over a 12-month period and can include a single Covered Data Transaction or be aggregated across Covered Data Transactions involving the same US Person and the same Foreign Person or Covered Person.

| US Sensitive Personal Data Category | Threshold of data collected about or maintained on more than |
|---|---|
| **Human genomic data** | 100 US Persons |
| **Human epigenomic data** | 1,000 US Persons |
| **Human proteomic data** | 1,000 US Persons |
| **Human transcriptomic data** | 1,000 US Persons |
| **Biometric identifiers** | 1,000 US Persons |
| **Precise geolocation data** | 1,000 US Persons |
| **Personal health data** | 10,000 US Persons |
| **Personal financial data** | 10,000 US Persons |
| **Covered personal identifier** | 10,000 US Persons |
| **Combined data (see below)** | 100,000 US Persons |

The bulk sensitive data threshold may be met through "combined data," which means any collection or set of data that contains more than one of the listed categories or that contains any listed identifier linked to the listed categories (except for the covered personal identifiers category) where any individual data type meets the threshold number of persons or devices collected or maintained in the aggregate for the lowest number of US Persons or US devices in that category.

Importantly, the regulated sensitive personal data under § 202.206 includes data that has been secured through various data protection techniques such as anonymization, de-identification, and encryption. Such techniques are relevant to certain exempt transactions contained in Subpart E and described below.

### 3. Access by a Country of Concern or Covered Person

Finally, the transaction must involve providing a Country of Concern or a Covered Person with "access" to the data at issue.

Notably, under § 202.201, "access" means either logical or physical access, including "the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information systems, information technology systems, cloud-computing platforms, networks, security systems, equipment, or software." In addition, for purposes of determining whether a transaction is a covered data transaction, access is determined without regard to the application or effect of any security requirements. For example, a transaction that provides a Country of Concern or a Covered Person access to data owned by a US Person and hosted by a US company on servers located in the US could still be subject to the restrictions of the DSP. Similarly, remote access to Covered Data by an individual in a Country of Concern or by a Covered Person may constitute a violation of the DSP rules. In short, the physical location of data inside the US is not sufficient to ensure compliance with the DSP.


## C. Examples of Prohibited and Restricted Transactions

The determination of whether a transaction meets the criteria described above requires a fact-specific analysis of the data sharing arrangement, the content and volume of the data to be shared, and the identity and location of the recipient party. As noted above, the regulations provide various examples to aid US Persons in this analysis. While there are too many scenarios to cover in this memorandum, a few basic examples of prohibited transactions include:

- A US company selling bulk US sensitive data to a company headquartered in a Country of Concern.
- A US company licensing bulk US sensitive personal data to a Covered Person.
- A US Person engaging in a vendor agreement with a Covered Person involving access to bulk US sensitive personal data.
- A US company providing access to Government-related Data or bulk US sensitive personal data to its IT employees in a Country of Concern.
- A US company contracting with an advertising vendor in a Country of Concern to track and process the US company's bulk US sensitive personal data.

# III. Authorization to Engage in Certain Restricted Transactions

Section 202.401 authorizes a US Person to engage in an otherwise restricted transaction involving a vendor agreement, employment agreement, or investment agreement with a Country of Concern or a Covered Person if the US Person protects the sensitive personal data in compliance with certain "Security Requirements" and complies with a variety of other measures. As set forth in § 202.248, the Security Requirements mean the Cybersecurity and Infrastructure Agency's (CISA) Security Requirements for Restricted Transactions, which include organizational-level, system-level, and data-level requirements for US Persons engaging in restricted transactions under the DSP. Persons engaged in restricted transactions must also implement a compliance program which adheres to DSP requirements regarding due diligence, audit requirements, recordkeeping, and other measures.

Companies relying on this authorization should be careful to ensure that their data protections meet the Security Requirements and that they have created and fully implemented a robust compliance program.

We note that this authorization could change depending on whether NSD continues to view it as serving the government's objectives. Accordingly, companies should be mindful that this authorization may not always be an available pathway for engaging in certain transactions and that its requirements could become more stringent over time.

Finally, the authorization is not applicable to data brokerage transactions or to transactions involving human 'omic data or human biospecimens from which such data can be derived, and which are subject to the prohibition in § 202.303.

# IV. Regulation of Data Brokerage Transactions with All Foreign Persons

The DSP also regulates certain data brokerage transactions with *all* foreign persons, even if they are not Covered Persons. Such transactions, while permissible, now involve new requirements under the DSP. Under the new rules, US Persons must, when conducting a data brokerage transaction with any foreign person, include contractual language precluding the foreign person from themselves providing the relevant data to Covered Persons or Countries of Concern. While the DOJ does not mandate specific language, examples of contractual clauses are included in the DOJ's Guidance.

Along with these requirements, DOJ recommends that US Persons subject to the DSP "maintain appropriate systems and controls, including reasonable and proportionate due diligence, to mitigate the risk they breach the DSP." In other words, it is not enough to simply rely on a contractual provision preventing data transfers by the foreign entity or person. Rather, US companies and individuals who share covered data with foreign individuals must "take reasonable steps to evaluate whether their foreign counterparties are complying with the contractual provision as part of implementing risk-based compliance programs" under the new rules. As discussed below, this puts new requirements on a significant number of US companies. In Part IX below, we provide an overview of how companies can work with counsel to best implement these changes.

# V. Licenses and Exempt Transactions

While the DSP's new rules are broad and complex, requiring US Persons to rigorously review their data transfer and storage policies, there are a number of exemptions to the DSP's prohibitions and restrictions. For example, there are exemptions for transactions that are 1) official business transactions of the US government; 2) transactions ordinarily incident to and part of financial services, including payment processing; and 3) corporate transactions that are part of business operations such as human resources, payroll, business travel, or customer support. However, the exemptions are narrow and will not apply to most business transactions involving Covered Data. We encourage companies and individuals to carefully review the rules — and consult with counsel — to see if any exemptions apply.

In addition, an otherwise prohibited transaction may be permissible if it falls under a general or specific license granted by NSD. Companies familiar with other US regulatory regimes, such as US economic sanctions, may recognize this dual-category license approach. A general license authorizes a particular type of transaction for a class of persons. General licenses are self-executing, meaning they allow persons to engage in certain transactions involving the US or US Persons without needing to apply for a specific license, provided the transactions meet certain terms and conditions as described in the general license. A general license is not specific to an individual or company but rather applies broadly to the general public.

A specific license, on the other hand, authorizes conduct by a specific person or defined group of persons and tends to relate to a narrow category of conduct that is relevant only to a small set of actors. NSD may issue a specific license to particular individuals or entities, authorizing a particular transaction or transactions in response to a written license application.

Because the DOJ has not historically acted as a regulator in this space, it remains to be seen whether NSD will regularly issue general licenses and, if so, what types of transactions will be permissible. As we have seen in other contexts (e.g., sanctions, export controls, etc.), applications for specific licenses can be a lengthy process.

# VI. New Requirements for US Persons and Companies

The DSP places new and potentially onerous responsibilities and requirements on US Persons whose activities may be implicated by the rules. They include:

## A. Due Diligence

The DSP Compliance Guide states that "U.S. persons must exercise due diligence to ensure and monitor compliance" with the new rules and "requires U.S. persons to reject participating in any transaction that violates the DSP, and to report such a rejected transaction" to the NSD. As discussed in more detail below, it is incumbent upon companies and individuals who already are, or may begin, engaging in Covered Data Transactions to work with counsel to put in place a fulsome compliance and due diligence program.

## B. Reporting

In addition to the annual reporting requirement described in Section F below, the DSP imposes an affirmative obligation on US Persons to file a report in the following circumstances:

- For a US Person engaging in a Covered Data Transaction with a foreign data broker, a report must be filed by the US Person when the US Person becomes aware of a known or suspected violation of the foreign data broker's contractual commitment to refrain from engaging in a subsequent Covered Data Transaction involving data brokerage of the same data with a Country of Concern or Covered Person (§ 202.302).
- For any US Person, a report must be filed after that US Person receives and affirmatively rejects an offer to engage in a prohibited transaction involving data brokerage (§ 202.1104).

In both circumstances, the US Person must file the report within 14 days of the triggering event.

## C. Record Keeping Requirements

The DSP also contains recordkeeping requirements. In sum, US Persons engaging in any transaction that is subject to the new rules must keep a full and accurate record of each transaction, and those records must be available for examination for ten years after the transaction is finalized. Importantly, recordkeeping requirements apply to Covered Data Transactions that are authorized by a general or specific license (with a few exceptions), meaning that even if a company has permission to engage in a covered transaction, it must maintain appropriate records for a decade.

For US companies engaged in restricted transactions, the rules also require a senior official at the US entity to sign an annual certification of the completeness and accuracy of the recordkeeping procedures, as confirmed by an audit (explained in more detail below).

## D. Compliance Program Requirement

Under the DSP, US Persons engaged in restricted transactions have an affirmative requirement to develop, implement, and routinely update an individualized, risk-based, written data compliance program. According to the DSP Compliance Guide, the failure to adopt and maintain adequate data compliance policies "is potentially a violation

of the DSP and may be an aggravating factor in any enforcement action." In other words, companies that do not institute a compliance program may risk stiffer penalties should the DOJ begin an enforcement action focused on a violation of the DSP's rules.

While acknowledging that every company has unique business interests and that each data compliance program will be different, the DSP Compliance Guide sets forth "minimum requirements" that every data compliance program should have. Those are:

- Establishing and implementing risk-based procedures for verifying data flows involved in any restricted transaction, including procedures to log, in an auditable manner: 1) the type of data at issue, 2) the identity of the transaction parties, including ownership or entities and citizenship or residence of individuals, and 3) the end-use of the data and method of data transfer.
- Screening all vendors to verify whether current or prospective vendors are Covered Persons under the DSP.
- A written policy that describes the data compliance program and its implementation, and is annually certified by an officer, executive, or other employee responsible for compliance.

The DOJ also states that data compliance programs should include a procedure for bringing newly acquired entities into compliance with the rules. This means that if your company acquires another entity, you must evaluate the new entity to ensure compliance with the DSP.

## E. Audit Requirements

As of October 2025, the DSP requires US Persons engaged in restricted transactions to audit their data compliance program, their compliance with the new rules, and all related software, systems, and technology. Each audit must specifically address the requirements set forth in the DSP. The rules require an audit once a year. Steptoe encourages clients to consult with counsel on how to best implement an effective audit program under the DSP.

## F. Annual Reporting Requirement

Certain US Persons engaged in cloud-computing services data transactions may be required to file an annual report describing such transactions engaged in during the previous calendar year. Such reports must be filed by March 1 of the year following the year of the report. This requirement, set forth in § 202.1103(a), applies to any US Person that is engaged in a restricted transaction involving cloud-computing services, and that has 25% or more of the US Person's equity interests owned (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise) by a Country of Concern or Covered Person.

## G. Training Personnel

The DSP Compliance Guide also suggests that companies consider providing periodic training on the DSP and its requirements for all relevant employees and personnel. While training on the DSP is not mandated under the rules, it is likely to be an important step in avoiding violations and mitigating penalties should an enforcement action be initiated.

# VII. Potential Civil and Criminal Liability

We expect that the Trump administration will prioritize enforcement actions against actors, including US Persons, who violate the new rules set forth in the DSP. NSD is authorized under the rules to bring civil enforcement actions and criminal prosecutions for knowing violations of the rules pursuant to the International Emergency Economic Powers Act (IEEPA), 50 USC. 1701, et seq. Importantly, "knowing" is not limited to actual knowledge and also includes situations in which a person reasonably should have known of the relevant facts that lead to a violation of the DSP.

Under IEEPA, violations of the rules are subject to civil penalties of up to the greater of $368,136 or twice the value of each transaction that violates the rules. With respect to criminal enforcement, willful violations of IEEPA, including violating the new DSP rules, are punishable by imprisonment of up to 20 years and a $1 million fine.

The rules also prohibit any activity that has the purpose of evading or avoiding the prohibitions set forth in the DSP, as well as any actions that cause or attempt to cause a violation of these prohibitions.

Similarly, it is a violation to knowingly direct a prohibited covered data transaction or restricted transaction (that does not comply with the requirements outlined above). Among other circumstances, the prohibition on knowingly directing such transactions is particularly important for US Persons that work for foreign companies, where the foreign company may not itself be directly subject to the DSP rules.

At this point, it is unclear how investigations and enforcement of DSP violations will proceed. NSD has both civil and criminal jurisdiction under the new rules to investigate, bring civil enforcement actions, and prosecute potential offenses. As enforcement begins, we will learn more about how civil regulators and criminal prosecutors will work together, whether authorities will primarily use administrative or grand jury subpoenas to acquire evidence, and whether US Attorney's Offices will be involved in enforcement. It is also possible that in the near future, we will see a parallel US Securities and Exchange Commission (SEC) enforcement regime with mandatory reporting requirements regarding DSP compliance for publicly traded companies.

# VIII. The DSP vs. PADFAA

It is important for industry to be aware that the restrictions and prohibitions under the DSP are distinct from those imposed by the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFAA). PADFAA, which took effect on June 23, 2024, generally makes it unlawful for a data broker to sell or otherwise make available personally identifiable sensitive data of a US individual to any foreign adversary country (China, Iran, North Korea, and Russia) or an entity that is controlled by a foreign adversary.

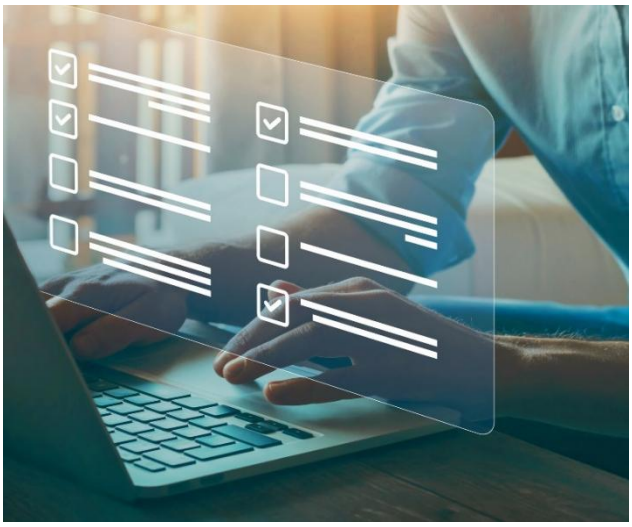
There are several key differences between PADFAA and the DSP, including:

- While the DSP covers six categories of sensitive personal data (described above), PADFAA generally covers broader types of

data, including photos, videos, recordings, private communications, information about minors, and certain intimate personal information.

- PADFAA only applies to the activities of third-party data brokers, but the DSP applies to classes of activities engaged in by any US Person.
- Unlike the DSP, PADFAA does not expressly address the reexport or resale of data by third parties or indirect sales through intermediaries to Countries of Concern.
- PADFAA permits the transmission of an individual's covered data with that individual's consent; there is no such "consent-exception" for the DSP.
- The Federal Trade Commission (FTC) is the agency tasked with bringing civil enforcement actions for any violations of PADFAA.

Accordingly, companies should be aware that the inapplicability of PADFAA does not mean that the DSP is also inapplicable, and vice versa. The same is true for compliance. Companies should evaluate their risks and responsibilities under these laws separately and tailor their compliance strategies to satisfy both sets of requirements, if applicable.



# IX. Assessing Risk and Implementing Compliance Measures

Until the DOJ establishes a pattern of enforcement actions for violations of the DSP, it is difficult to know which industries will be most impacted by the rules set forth in the DSP. However, any US company that stores, sells, or exchanges data with foreign individuals or companies must be aware of and come into compliance with the new rules. In particular, businesses in the artificial intelligence, financial services, information technology, healthcare, life sciences, and consumer sectors may have more exposure to the new rules than others due to the nature of their business operations and the sensitivity of their acquired and stored data. Even businesses that transact domestically may be subject to the DSP given its significant breadth and impact with respect to vendors, employees, and investors, in addition to data brokerage. Given the breadth of the new rules and the proliferation of data sharing in today's marketplace, we encourage companies to work with counsel to review the DSP and assess its impact on their business.

The prohibitions and regulations set forth in the DSP (with a few notable exceptions[1]) went into effect on April 8, 2025. The DOJ announced that it would begin enforcing the DSP on July 8, 2025, although it has yet to bring any enforcement actions as of October 2025.

Accordingly, companies whose activities may be impacted by the new requirements set forth in the DSP should begin efforts now to adjust business practices to comply with the rules. Some examples of steps to take include:

- Conduct internal data-mapping to determine if a company's activities fall under one of the categories of data that is subject to the DSP;
- Determine whether US sensitive personal data in the company's possession meets the "bulk" data thresholds under the DSP;
- Conduct a company-wide review to ensure knowledge of the location of and access to covered data, including the location of data servers;
- Evaluate all vendor agreements and pending contracts with vendors and other third parties to ensure that they are or will be in compliance with the DSP;
- Conduct due diligence on potential new vendors, including evaluating whether the new vendors engage in data brokerage business with Covered Persons or Countries of Concern, to ensure future compliance with the DSP;
- Negotiate contractual provisions with vendors and other third parties to ensure the data is not transferred to a Covered Person or Country of Concern, including provisions addressing downstream transfers of data;
- Consider conducting regular audits and employee training to ensure ongoing compliance with the DSP;
- Ensure that DSP requirements are evaluated as part of deal due diligence;
- Consider establishing a mechanism to track data transfers in real time to ensure compliance with the DSP;
- Evaluate the location of and relationship with board members who may be in Countries of Concern or be Covered Persons;
- Evaluate the location of IT and customer service workers and the data that is shared with those portions of the business;
- Consider whether adjustments to office locations or employee work locations, roles, or responsibilities are necessary to promote compliance;
- Evaluate presence in, relationship with, or contractual agreements with Covered Persons or Countries of Concern; and/or
- Consider whether an application for a specific license to engage in a Covered Data transaction would be in the interest of the company.

[1] The exceptions to the April 8, 2025, effective date are the affirmative obligations of subpart J (related to due diligence and audit requirements for restricted transactions), § 202.1103 (related to reporting requirements for certain restricted transactions), and § 202.1104 (related to reports on rejected prohibited transactions). Those obligations took effect on October 6, 2025.

The above list is non-exhaustive, and every company will have unique needs and activities and will require a holistic review of their business to determine how best to comply with the Data Security Program. Companies may leverage compliance efforts already undertaken, such as to comply with EU data protection rules, which notably impose the inventorying of personal data held and the mapping of data transfers.

The DOJ has made clear that if US Persons take affirmative steps, such as the ones described above, to comply with the new rules, regulators and prosecutors will look favorably on such actions should a violation occur. Similarly, the DOJ has emphasized the importance of voluntary self-disclosures in the white-collar crime context, and US Persons and counsel can expect that disclosure of DSP violations is also likely to be encouraged by authorities. On the other hand, if US Persons ignore or flout the rules, or try to evade enforcement, the DOJ has stated that this could potentially be an aggravating factor in any enforcement action. Indeed, the DOJ has emphasized that it will seek criminal enforcement in cases where individuals or companies willfully violate or attempt to evade or avoid the Data Security Program's requirements.

Steptoe, which offers combined experience in national security, DOJ investigations, and data protection is actively advising clients on compliance with the DSP rules. For additional information on the DSP or assistance in creating or implementing compliance programs, please contact a member of our team.

# Contacts


### Ross Weingarten
Partner
New York
+1 212 378 7628
rossweingarten@steptoe.com


Ross Weingarten, a partner in our New York office, is an experienced trial, white-collar criminal defense and regulatory investigations lawyer. He has led numerous high-stakes investigations and prosecutions across various sectors, showcasing his experience in handling complex legal matters.


### Anne-Gabrielle Haie
Partner
Brussels
+32 2 626 0502
aghaie@steptoe.com


Anne-Gabrielle Haie advises clients on a wide range of digital-related matters, with a strong focus on data protection, privacy and cybersecurity. In addition, she has developed considerable experience on AI and blockchain. She advises clients on compliance with EU laws and risk management. Anne-Gabrielle also has strong experience advising clients on data privacy and cybersecurity issues related to strategic transactions and commercial negotiations.


### Daniel W. Podair
Associate
New York
+1 212 378 7545
dpodair@steptoe.com


Daniel Podair focuses his practice on white-collar criminal defense, government and internal investigations, and complex civil litigation. Dan has significant experience representing clients in investigations and associated inquiries with government regulators, including the US Department of Justice and the US Securities and Exchange Commission, relating to securities, antitrust, and anti-corruption issues.


### Evan T. Abrams
Partner
Washington, DC
+1 202 429 3052
eabrams@steptoe.com


Evan Abrams counsels financial institutions, multinational corporations, and individuals on a variety of international regulatory and compliance matters. He regularly advises clients on issues related to anti-money laundering (AML), economic sanctions, export controls, foreign anti-corruption, the Committee on Foreign Investment in the United States (CFIUS), and the Defense Counterintelligence and Security Agency (DCSA).


### Andrew Adams
Partner
New York
+1 212 957 3081
acadams@steptoe.com


Andrew Adams advises companies and individuals in the areas of government and internal investigations, corporate governance, and white collar and regulatory matters. His practice includes a particular focus on anti-money laundering compliance, US economic countermeasures and national security crisis response, drawing on Andrew's time as the inaugural Director of the Department of Justice's Task Force KleptoCapture.


### Christian Auty
Partner
Chicago
+1 312 577 1293
cauty@steptoe.com


Christian Auty advises clients on the full lifecycle of data privacy and cybersecurity matters, from regulatory compliance and risk management to breach response and cross-border data governance, as well as on data privacy and governance considerations in emerging technologies such as artificial intelligence and blockchain.


### Quentin Johnson
Associate
Washington, DC
+1 202 429 6227
qjohnson@steptoe.com


Quentin Johnson assists clients on navigating US trade restrictions and national security laws, including economic sanctions, export controls, cybersecurity and data protection regulations, and customs laws. Quentin is a Certified Information Privacy Professional – US, and has advised clients on US cybersecurity and data protection laws, including FISA, CISA, ECPA, and the CLOUD Act.