PUBLICATION

DOJ Issues Additional Guidance and Clarification on the Bulk Data Transfer Rule: What U.S. Businesses Need to Know

Authors: Alexandra P. Moylan, Alisa L. Chestler, Michael J. Halaiko
April 22, 2025

On April 11, 2025, the Department of Justice's National Security Division (NSD) issued additional guidance to assist U.S. organizations in understanding and complying with the Data Security Program (DSP). As discussed in our prior alert, the DPS is a new regulatory framework codified at 28 CFR Part 202 (Final Rule). The Final Rule, which became effective in early April, prohibits or restricts certain transactions involving access by foreign adversaries in China, Russia, Iran, North Korea, Cuba, and Venezuela to "bulk" U.S. sensitive personal data and U.S. government-related data.

The DSP imposes what are effectively export controls that prevent foreign adversaries, and those subject to their control and direction, from accessing Americans' sensitive personal data (i.e., biometric, human omic, health, financial, and geolocation data, as well as data linked to current or former U.S. government employees or contractors) through various types of transactions, such as data brokerage, vendor agreements, employment agreements, and investment agreements. The DSP also requires U.S. entities engaged in certain transactions with foreign adversaries, known as restricted transactions, to comply with additional security, due diligence, auditing, and reporting requirements.

What U.S. Businesses Need to Know Regarding the NSD's Guidance Documents and Best Practices for Compliance during the DSP's Initial 90-day Period:

The Guidance includes three documents, (1) DSP Implementation and Enforcement Policy Through July 8, 2025 (2) DPS Compliance Guide, and (3) DSP Frequently Asked Questions.

It is important for U.S. businesses to know that compliance with DSP's requirements is required regardless of whether the bulk sensitive personal data is anonymized, pseudonymized, de-identified, or encrypted, which will be covered in a separate alert.

DSP Implementation and Enforcement Policy: Highlighting Good-faith Compliance Efforts

NSD recognizes that businesses must perform diligence to determine whether the DSP's prohibitions and restrictions apply to their activities and implement changes to their existing policies and processes for compliance. Depending on an entity's existing structure and commercial activities, compliance may require revising or creating new internal policies and processes, identifying data flows, renegotiating agreements, changing vendors or suppliers, adjusting employee roles or responsibilities, deploying new security requirements, and revising existing contracts.

NSD clarifies that DSP enforcement during the initial 90-day period will focus on egregious, willful violations so that the private sector can focus on compliance. The policy provides the following enforcement guidance for the initial 90-day period:

- NSD will not prioritize civil enforcement actions against any person for violations of the DSP that occur from April 8 through July 8, 2025, so long as the person is engaging in good faith efforts to comply with or come into compliance with the DSP during that time.

- The policy does not limit NSD's authority and discretion to pursue criminal enforcement in cases where individuals or entities willfully violate, attempt to violate, conspire to violate, cause a violation of, or engage in any action intended to evade or avoid the DSP's requirements.
- The policy provides the following examples of good faith compliance efforts:

1. Conducting internal reviews of access to sensitive personal data, including whether transactions involving access to such data flows constitute data brokerage;
2. Reviewing internal datasets and datatypes to determine if they are potentially subject to DSP;
3. Renegotiating vendor agreements or negotiating contracts with new vendors;
4. Transferring products or services to new vendors;
5. Conducting due diligence on potential new vendors;
6. Negotiating contractual onward transfer provisions with foreign persons who are the counterparties to data brokerage transactions;
7. Adjusting employee work locations, roles, or responsibilities;
8. Evaluating investments from countries of concern or covered persons;
9. Renegotiating investment agreements with countries of concern or covered persons; or
10. Implementing the Cybersecurity and Infrastructure Agency ("CISA") Security Requirements, including the combination of data-level requirements necessary to preclude covered person access to regulated data for restricted transactions.

DSP Compliance Guide: Highlighting Sample Contractual Language for Data Licensing

The Compliance Guide provides general information for compliance with the DSP's requirements. We are highlighting how NSD addresses one of the more broadly applicable legal requirements regarding common transactions, including the sale or licensing of regulated data. There are, however, various other topics addressed in the Compliance Guide to assist U.S. entities subject to the DSP in understanding the scope and purpose of the rule and their legal obligations.

DSP § 202.302(a)(1) requires certain contractual provisions for data brokerage transactions with foreign persons not covered by the DSP. Data brokerage means the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or vendor agreement, involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. The Final Rule does not define "sell" but through examples, it appears that there must be financial benefit or other valuable consideration exchanged to be "data brokerage."

An example of a transaction that falls within the scope of § 202.302(a)(1) is where a U.S. business knowingly enters into an agreement to sell bulk human genomic data to a European business that is not a covered person. Pursuant to the DSJ, in this situation, the U.S. business is required to include in that agreement a limitation on the European business' right to resell or otherwise engage in a covered data transaction involving data brokerage of that data to a country of concern or covered person. Otherwise, the agreement would be a prohibited transaction.

NSD's Compliance Guide provides the following sample contractual language for § 202.302(a)(1):

[U.S. person] provides [foreign person] with a non-transferable, revocable license to access the [data subject to the brokerage contract]. [Foreign person] is prohibited from engaging or attempting to engage in, or permitting others to engage or attempt to engage in the following: (a) selling, licensing of access to, or other similar commercial transactions, [such as reselling, sub-licensing, leasing, or transferring in return for valuable consideration,] the [data subject to the brokerage contract] or any part thereof, to countries of concern or covered persons, as defined in 28 CFR part 202; Where [foreign person] knows or suspects that a country of

concern or covered person has gained access to [data subject to the brokerage contract] through a data brokerage transaction, [foreign person] will immediately inform [U.S. person]. Failure to comply with the above will constitute a breach of [data brokerage contract] and may constitute a violation of 28 CFR part 202.

Additionally, the Compliance Guide suggests that U.S. businesses consider including contractual certification requirements requiring foreign persons to periodically certify their compliance with the required contractual restriction on onward transfer and to obligate the foreign person not to evade or avoid, cause a violation of, or attempt to violate any of the prohibitions set forth in Executive Order 14117 or 28 CFR part 202. The following sample language is provided:

[Foreign person] confirms that for [the brokerage contract], [foreign person] is in compliance with 28 CFR part 202 and any other prohibitions, restrictions[,] or provisions applicable to the [data subject to the brokerage contract]. [Foreign person] agrees to [periodically] certify to [U.S. person], in writing [foreign person's] compliance with 28 CFR part 202. [Foreign person] agrees to not evade or avoid, cause a violation of, or attempt to violate any of the prohibitions set forth in Executive Order 14117 or 28 CFR part 202]

The Compliance Guide emphasizes that U.S. businesses should not rely solely on contractual provisions or their foreign counterparties to comply with the DSP. Specifically, "NSD expects U.S. persons engaged in regulated data brokerage transactions to 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 proposed rule." We expect that this will entail not only initial steps towards compliance, but also ongoing diligence and potential auditing.

U.S. businesses will need to thoroughly evaluate their data and commercial activities to determine where § 202.302(a)(1)'s contractual language may be required and, even more importantly, when asked to agree to such language on its own behalf. The required language, along with the development and implementation of risk-based compliance programs, should be tailored to the business and its commercial activities.

Program FAQs

The Program FAQs answer 108 questions on various aspects of the DSP, such as the definitions, scope, applicability, exemptions, licenses, advisory opinions, and enforcement of the DSP. Most of the information is also contained in the preamble to the Final Rule, but the FAQ format presents a more streamlined and, therefore, simple format. NSD may update the FAQs based on additional questions received during the initial 90-day period.

The FAQs cover the following topics:

- ***Basic Program Information.*** The FAQs provide an overview of the DSP's purpose, effective date, enforcement policy, and interaction with other regulatory frameworks, such as the Committee on Foreign Investment in the United States (CFIUS), the Department of Commerce's Office of Information and Communications Technology and Services (ICTS), economic sanctions, and export controls.

- ***Definitions.*** The FAQs explain the key terms and concepts used in the DSP, such as U.S. person, country of concern, covered person, covered data transaction, government-related data, bulk U.S. sensitive personal data, data brokerage, vendor agreement, employment agreement, investment agreement, access, and security requirements.

- ***Scope and Applicability.*** The FAQs clarify the types of transactions and data subject to the DSP's prohibitions and restrictions, as well as the types of transactions and data that are outside the scope

of the DSP or exempt from its requirements. The FAQs also address some common scenarios and examples of how the DSP may apply to different situations and industries, including research, education, health care, financial services, telecommunications, and cloud computing.

- ***Exemptions.*** The FAQs provide more details on the types of transactions that are exempt from the DSP's prohibitions and restrictions, such as transactions involving official business of the U.S. government, financial services, corporate group transactions, transactions required or authorized by federal law or international agreements, telecommunications services, and certain drug, biological product, and medical device authorizations. The FAQs also explain the recordkeeping and reporting requirements that apply to some of these exempt transactions.

- ***Licensing.*** The FAQs describe the difference between general and specific licenses and the process and criteria for applying for a specific license. The FAQs also state that NSD applies a presumption of denial standard for all license applications. "To overcome this presumption, a license application will need to affirmatively identify compelling countervailing considerations to support the issuance of a specific license (such as an emergency or imminent threat to public safety or national security)."

- ***Compliance Requirements.*** The FAQs provide guidance on how U.S. entities can comply with the DSP, including the prohibitions, restrictions, exemptions, licenses, and compliance program requirements. The FAQs also address some issues related to the security, due diligence, auditing, recordkeeping, and reporting requirements for certain transactions, as well as the role and responsibilities of senior management and compliance personnel.

- ***Enforcement Guidance.*** The FAQs provide information on the penalties, liability, and enforcement actions for violations of the DSP, as well as the factors that NSD may consider in determining whether to pursue enforcement or grant mitigation. Violations of DSP may result in civil and/or criminal penalties "which can be substantial" including civil penalties "not to exceed the greater of $368,136 or an amount that is twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed". The FAQs also explain how U.S. entities can voluntarily self-disclose or report possible violations of the DSP, and how they can cooperate with NSD investigations.

For more information or assistance on this topic, please contact Alexandra P. Moylan, CIPP/US, AIGP, Alisa L. Chestler, CIPP/US, QTE, Michael J. Halaiko, CIPP/E, or another member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.