Articles + Publications | April 16, 2025

DOJ's Latest Guidance on the Data Security Program – What's New?

WRITTEN BY

Peter E. Jeydel | James Koenig | David J. Navetta | Ronald Raether, Jr. | Laura Hamady

The new Department of Justice (DOJ) Data Security Program (DSP) took effect on April 8. For an overview of the DSP, see our earlier advisory and recent update.

On April 11, DOJ's National Security Division (NSD), which administers the DSP, issued an array of detailed guidance about how the DSP will work, including a Compliance Guide, Frequently Asked Questions (FAQs), and an Implementation and Enforcement Policy that provides a 90-day leniency period for civil enforcement through July 8. DOJ has signaled its intent to issue more extensive enforcement guidance and to populate the Covered Persons List soon.

While the full DSP compliance and enforcement structure remains a work in progress, the DOJ's most recent guidance provides invaluable insight for organizations monitoring their compliance obligations. We highlight the key takeaways below.

The 90-day leniency period is an opportunity to establish full compliance with the DSP

To dispel any misconceptions around the leniency period, it is clear from Deputy Attorney General Todd Blanche's statement accompanying the DOJ's recent guidance that the Trump administration has embraced the DSP as an integral part of carrying out its policy priorities. The DSP will continue to evolve, but there is no indication that it is going away or will be watered down. The DOJ appears to be fully committed to pushing the program forward and has called it "urgent," explaining that this leniency period is about giving time both for industry and government to get it right.

Since the DSP's April 8 effective date, compliance with the DSP has been required, except for specific due diligence, audit, and reporting requirements for restricted transactions, and reporting on rejected prohibited transactions. These additional obligations take effect on October 6 and are unaffected by the leniency period.

So what's the leniency period all about? In essence, it is a limited non-enforcement policy for civil violations until July 8 that is heavily caveated, as follows:

NSD will target its enforcement efforts during the first 90 days to allow U.S. persons (e.g., individuals and companies) additional time to continue implementing the necessary changes to comply with the DSP and provide additional opportunities for the public to engage with NSD on DSP-related inquiries. Specifically, 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…

At the same time, during this 90-day period, NSD will pursue penalties and other enforcement actions as appropriate for egregious, willful violations. This policy does not limit NSD's authority and discretion to pursue civil enforcement if such persons did not engage in good-faith efforts to comply with, or come into compliance with, the DSP…

At the end of this 90-day period, individuals and entities should be in full compliance with the DSP and should expect NSD to pursue appropriate enforcement with respect to any violations.

The key caveats here are: 1) the leniency only applies to those that are engaged in good faith efforts to comply, 2) accordingly, criminal enforcement will continue, and even civil enforcement is a possibility for those not moving toward full compliance in good faith, and 3) by July 8, full compliance is expected (subject to the delayed October 6 effective date for certain elements, as noted above).

Standard contractual language

In the Compliance Guide, DOJ has provided suggested language that can be used in situations of data brokerage with non-covered foreign persons (*i.e.*, counterparties in third countries without the types of links to China or other "countries of concern" that trigger most of the DSP's restrictions and prohibitions). The suggested language is:

[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.

DOJ has also indicated that additional language may be warranted in some cases, including the following certification:

[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.

DOJ has made it clear that using this particular language is not necessarily required, and that it can be modified.

Indeed, we expect that some organizations will want to adjust this language to fit their particular circumstances. One question that will come up with respect to the proposed certification is what exactly the foreign person is agreeing to when it comes to "complying" with the DSP regulations, which generally apply only to U.S. person activities — DOJ's intentions there are less than clear, in particular when it comes to vendor, employment and investment agreements (*i.e.*, covered transactions that are not "data brokerage").

Where particular elevated risks are present, tailored language around those risks may be prudent. But this template language offers a useful starting point that has been endorsed by DOJ.

General compliance expectations

Contractual language alone is generally not a sufficient compliance approach under the DSP. DOJ points to this in the Compliance Guide when it notes that the compliance steps organizations may need to take during this 90-day leniency period include "changing vendors or suppliers," "adjusting employee work locations, roles or responsibilities," and "renegotiating investment agreements." The requirements for restricted transactions in particular are extensive and go far beyond just adding standard contractual clauses.

Even in situations of data brokerage with non-covered foreign persons, when the contractual language above is to be used, DOJ has emphasized that merely using this contractual language is not sufficient:

Notwithstanding the use of any such clauses, U.S. persons subject to the DSP must still maintain appropriate systems and controls, including reasonable and proportionate due diligence, to mitigate the risk they breach the DSP. U.S. persons engaged in these kinds of data brokerage transactions with non-covered foreign persons and third countries should not simply shift responsibility to or entirely rely on the contractual provisions or on their foreign counterparties to comply with these contractual provisions.

A risk-based compliance program is what DOJ will look for, informed by the traditional expectations that apply under other regulatory regimes based on the International Emergency Economic Powers Act (IEEPA), such as U.S. economic sanctions. As an illustration, DOJ indicated that in some cases inadequate risk-based controls such as due diligence may itself constitute prohibited "evasion" of these regulations.

The takeaway is that the DSP is generally not a mere "paper compliance" regime, where simple steps like obtaining consents or putting in place contractual provisions will satisfy the requirements. Rather, for many organizations impacted by these new rules, substantial changes in business practices (including with respect to employees, systems, etc.) and vendor and investor relationships may be needed.

Notably, the DOJ's Compliance Guide suggests that organizations that deal with covered data under the DSP should implement a risk-based compliance program, even if they believe that ultimately they may not engage in any covered data transactions, or that all such transactions will fall under one or more of the DSP's exemptions. With that said, when the DSP has limited applicability to a particular organization, the compliance approach may be narrowly tailored accordingly. For example, DOJ's Compliance Guide indicates that in some cases organizations should convey the requirements of their compliance program to third parties and even offer training to third parties. With such high expectations on the part of the government in certain instances, it will be important to have a solid understanding of how to appropriately tailor a compliance program based on an organization's risk

exposure, so the government can be satisfied without undue cost or operational disruption.

Gray areas and ambiguities – how to navigate the DSP

DOJ has issued reams of information about the DSP during the notice and comment rulemaking process, in public remarks and private engagements, and with this new guidance. But the agency has not yet clarified some of the toughest issues that organizations will face under the DSP. Moreover, several statements the DOJ has issued in recent months may appear confusing or even contradictory.

It will be critical for organizations with exposure to these regulations to chart a clear path through these murky areas based on a comprehensive understanding of the DSP and how DOJ will enforce it. We provide a few illustrations below.

Audits

The Compliance Guide includes the potentially misleading statement that, "[t]o detect compliance gaps, U.S. persons must audit their Data Compliance Program." However, audits are not required in all circumstances. Further compounding the confusion, the Compliance Guide states that those conducting required audits under the DSP "should not be involved in the transaction or associated with, owned, or controlled by any person who is party to or otherwise involved in the transaction they are auditing." That could easily be misinterpreted to mean that internal audit personnel cannot be used for this purpose. However, the rulemaking that established the DSP and the recent FAQs both say the opposite (although with some heavy words of caution about relying on internal auditors), and the regulations were modified explicitly for the purpose of allowing internal audits. These is just an example of how easy it can be to become misled and confused about what the real obligations and expectations are under the DSP.

Recordkeeping

Additionally, the DSP has a broad 10-year recordkeeping requirement that will be highly burdensome for many organizations, and DOJ has made somewhat unclear statements about its applicability. For example, DOJ has said that, "[e]xcept as otherwise provided, U.S. persons engaging in any transaction subject to the DSP must keep a full and accurate record of each such transaction …". However, the DSP's broad recordkeeping requirements actually only apply in limited cases; for example, they are not applicable when operating pursuant to most of the exemptions.

Still, organizations impacted by these rules should consider keeping affirmative compliance records as a protective measure, even when not required, because DOJ has broad subpoena authority under the DSP — the FAQs that were just issued state that DOJ has the authority "to request and subpoena information to the fullest extent permitted by law, including, as appropriate, regarding transactions that may ultimately be exempt under the DSP." So, even though broad recordkeeping is not strictly required under most of the exemptions, some recordkeeping would be prudent.

Domestic activity

Another tricky area is to what extent organizations can focus their compliance efforts on data flows outside the U.S., as opposed to purely domestic activity. In general, the DSP does not apply to activity that takes place entirely within the U.S. But DOJ has set out a few limitations to that general rule.

The clearest exception is when an individual or entity is specifically designated by DOJ on the DSP's Covered Persons List (which again is not yet populated but will be soon) – those parties are "covered persons" even when located in the U.S. DOJ has even stated in the Compliance Guide that a "U.S. person [which DOJ has defined to include any person in the U.S.] is *never* a covered person unless designated as such by" DOJ on the Covered Persons List (emphasis added). But other DOJ statements could be viewed as possibly contradicting that — for instance, one of the examples under the definition of U.S. person in the DSP regulations states that a U.S. branch of an entity based in a country of concern such as China is a foreign person and therefore a covered person, even though a U.S. branch is by definition in the U.S.

This could cause some organizations to consider conducting due diligence for any covered transactions involving U.S. branches of entities based in China or other countries of concern, although other organizations may determine on a risk basis that this is not necessary.

Enhanced due diligence

DOJ has indicated that organizations may need to conduct due diligence on the individual representatives (*e.g.*, executives) of organizations with which they conduct covered transactions, in order to assess if the individuals are covered persons even when their organizations are not covered persons. This is a familiar concept to those accustomed to U.S. economic sanctions compliance expectations, but can be challenging in practice when screening and due diligence procedures are focused on the entity counterparty. Accordingly, this type of due diligence and screening can be conducted as a function of risk and does not necessarily have to be done in all cases.

DOJ has emphasized repeatedly that the general rule in this context is that U.S. persons are not expected to conduct such "second-level" due diligence on the employment practices of foreign persons that are counterparties in covered data transactions to determine whether the foreign person's employees qualify as covered persons.

Similarly, when entities that are not covered persons are controlled by, or minority-owned by, covered persons, DOJ has laid out an expectation that tracks with compliance principles under U.S. economic sanctions. While such control or minority ownership on its own does not cause these entities to be covered persons, DOJ has issued the following cautionary words:

A covered person holding a controlling interest may present risks of access, which is why control is one of the criteria for NSD to consider when designating an entity as a covered person under § 202.211(a)(5) [i.e., the Covered Persons List] *if such an entity is determined to meet the relevant criteria. U.S. persons should exercise caution when considering engaging in covered data transactions with an entity that is not a covered person but in which one or more covered persons have significant ownership that is less than 50%, or which one or more covered persons may control by means other than a majority ownership interest. Ownership percentages can fluctuate such that an entity could become a covered person, and such entities may be designated by NSD based on the significant controlling interest. Additionally, persons should be cautious in dealing with such an entity to*

ensure that they are not engaging in evasion or avoidance of the DSP.

This warning indicates that there are circumstances when due diligence should go beyond the counterparty and its 50% or majority owners, to include minority owners, control parties, and any individual whose involvement may provide access to covered data (along with the representatives of an organization who are directly involved in the transaction, as discussed above). When such enhanced due diligence is warranted is, again, a risk-based judgment call that can be informed by trends seen in analogous regulatory programs under IEEPA.

Takeaways

The points above are meant to illustrate just a few of the nuances and complexities that organizations will confront under the DSP and to emphasize the value of seeking out qualified guidance to help navigate this highly complex, and still new and evolving, regulatory program. It is critical to craft a compliance approach under the DSP that is based on a thorough understanding of the rules, and, perhaps equally important, how DOJ is likely to enforce the rules in light of its policy objectives, resources and priorities, and the lessons that can be drawn from the enforcement trends we have seen in recent years under similar regulatory regimes such as economic sanctions.

When/how to engage with DOJ

Many organizations will have questions about the DSP during this 90-day leniency and compliance period, such as how they should grapple with specific gray areas, how the regulations apply in niche cases, and whether they can obtain authorization to engage in activity that may not be feasible to shift into full compliance with the DSP by July 8.

In terms of formal advisory opinion and license requests, DOJ has indicated those will generally need to wait:

NSD discourages the submission of any formal requests for specific licenses or advisory opinions during this 90-day period: Although requests for specific licenses or advisory opinions during this 90-day period can be submitted, NSD will not review or adjudicate those submissions during the 90-day period (absent an emergency or imminent threat to public safety or national security) …

Furthermore, license requests will be subject to a "presumption of denial" standard, which is a high hurdle to overcome. DOJ has stated that obtaining a license will require the applicant "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)." Mere commercial interests may not suffice, unless a strong showing can be made that there are broader implications relating to the public interest.

While DOJ is open to informal questions, they have issued several warnings that these communications may not be treated as confidential (and could even potentially be used for enforcement purposes), so caution is warranted.

When violations are identified, organizations should consider submitting voluntary self-disclosures (VSDs). At this stage, DOJ has only issued preliminary guidance about VSDs under the DSP, including stating that "NSD may consider a qualifying voluntary self-disclosure as a mitigating factor in any enforcement action, which may result in a reduction in the base amount of any proposed civil penalty." DOJ has stated that they will take an approach to

the VSD process under the DSP that aligns in certain ways with the process under the U.S. Export Administration Regulations (EAR), with an initial notification followed by a full report within 180 days. DOJ has indicated they may issue more robust VSD guidance in the future, but in the meantime one can look to other analogous DOJ VSD policies for principles that may apply under the DSP, in particular where there may be criminal exposure (which notably the guidance referenced above did not mention). Organizations that believe they may have engaged in violations of the DSP should take lessons from other IEEPA-based regulatory regimes to engage in a careful evaluation of the pros and cons of submitting a VSD.

Importantly, DOJ has confirmed that the FinCEN whistleblower program covers the DSP, which presents opportunities for individuals who are aware of violations in which they were not significantly involved, but poses significant risks for organizations.

Conclusion

While there are answers to some of the key questions under the DSP, the reality is that many of the gray areas we see today will persist for some time. Counsel with deep experience in risk-based compliance under similar regulatory regimes based on IEEPA can assist with shaping a compliance approach that is neither overinclusive nor underinclusive, and that balances feasibility with satisfying DOJ's expectations.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber
- Sanctions + Trade Controls
- White Collar Litigation + Investigations