COVINGTON

DOJ Releases Guidance Regarding Implementation of Bulk Sensitive Data Executive Order

ALERT

APRIL 15, 2025

On April 11, 2025, the U.S. Department of Justice ("DOJ") **released** guidance regarding implementation of Executive Order 14117, "**Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern**" (the "EO"). The **final rule** implementing the EO (the "Final Rule") took effect on April 8, 2025. The Final Rule, which DOJ **calls** the "Data Security Program" or "DSP" "establishes what are effectively export controls that prevent foreign adversaries, and those subject to their control, jurisdiction, ownership, and direction, from accessing U.S. government-related data and bulk genomic, geolocation, biometric, health, financial, and other sensitive personal data." As discussed in our previous analysis of the Final Rule, under the DSP, certain "covered data transactions" with "countries of concern" (China, Cuba, Iran, North Korea, Russia, and Venezuela) or "covered persons" are prohibited. Other types of covered data transactions may proceed, but only if U.S. persons party to such transactions first implement the "Security Requirements" issued by the U.S. Cybersecurity and Infrastructure Security Agency ("CISA") and implement additional compliance measures contemplated by the DSP.

DOJ issued three documents: an **Implementation and Enforcement Policy**, a **Compliance Guide**, and an initial **Frequently Asked Questions** ("FAQs") document. Below we summarize the key elements of these documents.

Implementation and Enforcement Policy

In its Implementation and Enforcement Policy, DOJ stated that it "recognizes that individuals and companies may need to take steps to determine whether the DSP's prohibitions and restrictions apply to their activities, and to implement changes to their existing policies or to implement new policies and processes to comply." DOJ further stated that it "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." DOJ offered the following examples of good-faith 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;
- Renegotiating investment agreements with countries of concern or covered persons; or
- Implementing the [CISA] Security Requirements, including the combination of data-level requirements necessary to preclude covered person access to regulated data for restricted transactions."

However, the policy is also clear that DOJ may still, during this 90-day period, pursue "penalties and other enforcement actions as appropriate for egregious, willful violations." For instance, DOJ could pursue civil enforcement against persons who "did not engage in good-faith efforts to comply with, or come into compliance with, the DSP." DOJ could also 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." Thus, although the policy is intended "to allow the private sector to focus its resources and efforts on promptly coming into compliance and to allow [DOJ] to prioritize its resources on facilitating compliance," DOJ signaled that it may still pursue certain violations inconsistent with the purposes of the announced delay in civil enforcement.

Further, DOJ explained that at the end of the 90-day period, full compliance with the DSP is expected, and individuals "should expect [DOJ] to pursue appropriate enforcement with respect to any violations." It also is important to note that even the 90-day period of deprioritized civil enforcement is merely a statement of how DOJ intends to exercise its discretion, and not a formal suspension of the Final Rule's requirements or a binding commitment not to pursue enforcement cases.

Compliance Guide

DOJ also issued a DSP Compliance Guide, which covers a number of topics, ranging from sample contractual language and suggestions for what a U.S. person may incorporate into its Data Compliance Program, to the temporary delay on the consideration of specific licenses (other than emergency situations) and possible forthcoming guidance.

Sample Contractual Language for Data Brokerage with Foreign Persons That Are Not Covered Persons

The DSP **requires** that U.S. persons engaged in covered data brokerage transactions with foreign persons who are not covered persons "[c]ontractually require[] that the foreign person refrain from engaging in a subsequent covered data transaction involving data brokerage of the same data with a country of concern or covered person" in order to proceed with the covered data transaction. While the Compliance Guide notes there is no specific contractual language that must be included, it offers sample contractual language for parties considering such engagements:

> *"[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."

Of note, this contractual language goes a step further than the DSP's requirement, introducing a reporting requirement for the *foreign person* to notify the U.S. person regarding any known or suspected access by a country of concern or covered person.

The Compliance Guide also proposes contractual language for an annual certification by the foreign person that the foreign person remains in compliance with the DSP and that the foreign person will not "evade or avoid, cause a violation of, or attempt to violate any of the prohibitions" of the DSP. While certain of these proposed contractual requirements are not explicitly required by the DSP, they may serve to indicate how DOJ will assess whether U.S. persons have undertaken "reasonable steps" to ensure a foreign person counterparty's compliance with the contractual provisions.

Data Compliance Program

U.S. persons who engage in restricted transactions must implement a Data Compliance Program as part of so-called "know-your-data-requirements." The Compliance Guide emphasizes the importance of "adequate data compliance policies and procedures" and that a lack of such policies may constitute "an aggravating factor in any enforcement action." While noting that such programs should be designed based on the U.S. person's risk profile, DOJ offered some insights into what such a program *could* look like, including verifying the types and volumes of data involved in a transaction, the identity of the parties to the transaction, and the data's end-use.

With respect to due diligence, the Compliance Guide suggests as a "best practice" that the U.S. person conduct regular risk assessments to help design the compliance program, noting that, "ideally," such risk assessments should occur at least annually. DOJ noted that the following could be part of the risk assessment:

- the company's current security measures,
- the company's employees, vendors, and investors,
- the company's offered products and services,
- the company's coverage under existing licenses or exemptions, and
- the geographic locations of the company and its subsidiaries, parent organizations, vendors, intermediaries, and counterparties.

The Compliance Guide also proposes ideas for vendor management and validation processes, such as suggesting that screening software should:

- "incorporate[] updates to the Covered Persons List,"
- "account[] for all identifiers, including alternative spellings or AKAs of identified or designated covered persons,"
- "account[] for organizational hierarchy,"
- "consider[] vendors' geographical information (including headquarters, subsidiary, and branch locations)[,] and"

- "screen[] against both current, newly added, and prospective vendors."

The Compliance Guide further suggests that U.S. persons should provide Data Compliance Program and CISA Security Requirements training "to all relevant employees and personnel," offering several ideas regarding what could be included in such a training program. DOJ also recommended the inclusion of internal controls that enable organizations to "identify, escalate, and report . . . any covered data transaction that may violate the DSP" to appropriate personnel, and take steps to remediate any deficiencies identified by an audit.

Licensing

U.S. persons seeking to engage in certain covered data transactions that otherwise would be prohibited may seek a specific license to engage in such a transaction. However, DOJ stated that it will apply a "'presumption of denial' standard for all specific license applications," and that overcoming the presumption generally will require an affirmative showing of "compelling countervailing considerations" (*e.g.*, "an emergency or imminent threat to public safety or national security").

Furthermore, DOJ "will not review or adjudicate [any requests for specific licenses submitted] during the [first] 90-day period (absent an emergency or imminent threat to public safety or national security)." Instead, DOJ encouraged the submission of informal inquiries regarding the DSP and recently released guidance materials during this 90-day period.

Possible Additional Forthcoming Guidance

Of note, DOJ stated that it may provide "DSP Enforcement Guidance" that offers information regarding Voluntary Self-Disclosure ("VSD") programs. Forthcoming DSP Enforcement Guidance may also include what is considered a "transaction" under the calculation of penalties.

Frequently Asked Questions ("FAQs")

DOJ also issued responses to more than 100 FAQs. Some of the responses provided additional clarity:

- The FAQs state that for purposes of determining which transactions are covered by the DSP, "U.S. persons should only consider covered data transactions 'in the preceding twelve months' that occur on or after the effective date of the DSP." Thus, for purposes of determining whether the "bulk" threshold has been met, persons need only look at the transactions conducted on or after April 8, 2025.
- The FAQs indicate the independence of an audit may be determined based on a number of factors such as:
  - "the U.S. person's internal corporate structure,"
  - "the internal auditor's accountability to senior leadership and/or the U.S. company's board of directors," and
  - "the training and expertise possessed by the internal auditor."
  - The FAQs note that DOJ intends to issue further information regarding "the requirements for a sufficiently independent audit."
- DOJ confirmed that audit reports may be used as evidence in an enforcement action if the audit report "demonstrates a company's failure to comply with the DSP."
- DOJ noted that an advisory opinion may be revoked at any time, without initial public notice.

That said, the FAQs largely reiterate the language of the Final Rule and do not address many of the less clear aspects of the Final Rule that have generated confusion. For example:

- DOJ did not provide any guidance regarding the scope of the exclusion for passive investments, including whether a direct investment in a privately held entity, that is otherwise strictly passive and below 10 percent, would be excluded.
- DOJ reiterated that anonymized, deidentified, pseudonymized, and aggregated data fall within the definition of bulk U.S. sensitive personal data, but did not further explain what any of these terms mean.
- DOJ did not offer a specific requirement for how often vendors, employees, and investors must be screened, but noted that the screening frequency "must be guided by your organization's internal policies and procedures, based on [the company's] risk profile."

If you have any questions concerning the material discussed in this client alert, please contact the members of our CFIUS practice.

Related Professionals

David N. Fagan

PARTNER

+1 202 662 5291

dfagan@cov.com

Heather L. Finstuen

PARTNER

+1 202 662 5823

hfinstuen@cov.com

Mark E. Plotkin

PARTNER

+1 202 662 5656

mplotkin@cov.com

Jonathan R. Wakely

PARTNER

+1 202 662 5387

jwakely@cov.com

Julia F. Post

OF COUNSEL

+1 202 662 5249

jpost@cov.com

Ingrid Price

SPECIAL COUNSEL

+1 202 662 5838

iprice@cov.com

Janine N. Slade

SPECIAL COUNSEL

+1 202 662 5239

jslade@cov.com

Brian S. Williams

OF COUNSEL

+1 202 662 5270

bwilliams@cov.com

Lawrence Barker

ASSOCIATE

+1 202 662 5437

lbarker@cov.com

Alexandra Bruer

ASSOCIATE

+1 202 662 5588

abruer@cov.com

Corinne Cook

ASSOCIATE

+1 202 662 5077

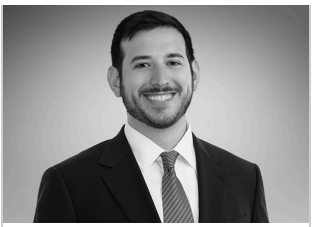
ccook@cov.com

Jacob T. Crump

ASSOCIATE

+1 202 662 5591

jcrump@cov.com



Sam Karson

ASSOCIATE

+1 202 662 5341

skarson@cov.com

Brian J. Kim

ASSOCIATE

+1 202 662 5703

bkim@cov.com

Monty Roberson

ASSOCIATE

+1 202 662 5903

mroberson@cov.com

Madeline E. Sanderford

ASSOCIATE

+1 202 662 5408

msanderford@cov.com

Related Practices

Regulatory and Public Policy

CFIUS

COVINGTON