GOODWIN

ALERT · APRIL 4, 2025

DOJ's Data Export Rule Is In Force April 8: What You Need to Do

BY Omer Tene Justin C. Pierce Federica De Santis Gozde Guckaya

On April 8, 2025, a sweeping rule issued by the US Department of Justice (DOJ) will take effect. The rule imposes restrictions—and in some cases, outright prohibitions—on US companies in connection with certain types of data brokerage vendor relationships, employment arrangements, and investment agreements involving six "countries of concern" and individuals or entities linked to them: China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela.

For additional background on the rule, please see our prior client alert.

The rule, which the DOJ may enforce through civil or criminal penalties, applies to a broad range of US companies, including those that rely on vendors, cloud providers, tracking technologies, or employees based in countries of concern. Even indirect access to sensitive data by a covered person may trigger compliance obligations or prohibitions.

Importantly, unlike traditional privacy laws, including even the EU's strict data transfer restrictions, the rule applies to transfers of, or potential access to, even de-identified or anonymized data. While robust de-identification or anonymization may be sufficient to exempt some data transactions related to clinical studies and regulatory approvals in a country of concern, such transfers or access remain subject to the rule and additional reporting and recordkeeping obligations.

US companies should now take steps to evaluate whether their data practices, third-party relationships, or ownership structures bring them within the scope of the rule. Certain covered data transactions will be *prohibited* on April 8, 2025; others will be *restricted*, that is barred absent implementation of the specified "security requirements" published by the Cybersecurity and Infrastructure Security Agency (CISA). Additional due diligence, reporting, and auditing requirements are delayed until October 6, 2025.

The checklist below is intended to help organizations make an initial assessment. While the rule also restricts the transfer of US government-related data, this checklist focuses on transactions involving US sensitive personal data, which have the potential to affect many businesses in the United States.

1. Sensitive Data Volume

Do you collect or handle a large volume of (referred to in the rule as "bulk") sensitive personal data—such as human genomic or omic data, biometric identifiers, precise geolocation data, health records, financial account information, or covered personal identifiers—about US persons? See the Appendix in our prior client alert for further detail and bulk thresholds for US sensitive personal data.

If yes, you likely hold "bulk" sensitive personal data covered by the rule.

2. Foreign Access
Do any ”covered persons” have access to the bulk US sensitive personal data you hold—or to the systems that house the data? This includes entities that are organized or have their principal place of business in a country of concern, individuals primarily resident in a country of concern, individuals employed by a covered person, individuals or entities identified on a forthcoming Covered Persons List, and entities that are owned 50% or more by another covered person.

If yes, you may be engaged in a covered data transaction subject to the rule.

3. Prohibited Data Sales/Sharing
Are you selling, licensing, or otherwise sharing bulk US sensitive personal data—directly or indirectly (e.g., through third-party analytics or advertising tools)—to a covered person or country of concern? For example, does your app send user data to a platform based in China?

If yes, the rule *prohibits* data brokerage—the sale or licensing of covered data to a country of concern or covered person where the recipient did not collect the data directly. Prohibited transactions, such as these, do not benefit from exceptions or mitigation through cybersecurity controls, and should be identified and restructured or terminated as appropriate.

Notably, the DOJ’s definition of data brokerage is broader than that found in existing state data broker laws. While state laws typically apply only to businesses that sell personal data they did not collect themselves, the rule applies even where companies are selling or licensing first-party data—i.e., data they collected themselves.

4. Contractual Safeguards for Data Brokerage with Other Foreign Partners
Do you sell, license, or otherwise share bulk US sensitive personal data with any non-US entities *outside* the listed countries (e.g., European or Canadian processors or affiliates)?

If so, you must include contractual provisions that prohibit them from transferring the data to covered persons or countries of concern and require them to notify you of any unauthorized transfer. If not, your agreements may not meet the rule’s requirements.

5. Human Genomic or other Human ‘omic Data Exports
Do you collect or transfer genetic or human ‘omic data—or biospecimens from which such data can be derived—to any covered person or to any company, lab, or individual linked to a country of concern? For example, are you sharing US biosamples, from which DNA sequence data can be extracted, with a business or research partner in China?

If yes, these transfers may be prohibited under the rule.

6. Foreign Vendors/Services
Do you rely on vendors or service providers (e.g., cloud hosting, IT support, or data analytics) based in countries of concern for services that involve access to bulk US sensitive personal data?

If yes, the rule categorizes the arrangement as a restricted transaction, which is only permitted if you implement robust data security measures that comply with DOJ and CISA requirements. Covered data transactions involving human ‘omic data or data derived from human biospecimens may be prohibited.

7. Employees/Contractors Abroad
Do you have employees or contractors in countries of concern who can access your systems or view bulk US sensitive personal data?

If yes, this is a restricted transaction requiring strong cybersecurity policies, access controls, and auditing procedures—or a prohibited transaction if involving human ‘omic or biospecimen data.

8. Investors/Partners from Abroad
Do you anticipate any investment-type agreements or arrangements that will result in a covered person receiving an equity

interest in a US entity (e.g., investment from a Hong Kong-based venture capital fund)?

If yes, this should be analyzed under the rule (and under the CFIUS regulations). Some investments may be exempt as “passive investments” while others may proceed as a restricted transaction, assuming compliance with the rule’s safeguards. Non-passive investments into US companies that hold bulk US sensitive personal data in the genomic or human ‘omic categories may be prohibited.

9. Applicable Exemptions
Do any of your data transfers qualify under an exemption—such as those related to public health reporting, law enforcement, or FDA-regulated clinical research?

If yes, you may be exempt from the rule’s restrictions. However, note that individual consent is not a valid exemption—you must rely on one of the specific exceptions recognized by the rule. Moreover, some exempted transactions remain subject to reporting and recordkeeping requirements set forth in the rule.

Conclusion

With the April 8 effective date fast approaching, US companies should promptly assess their cross-border data practices, vendor relationships, and potential foreign investments to determine whether they are subject to the DOJ’s rule. Early identification of covered or restricted transactions will be critical to avoiding compliance failures and ensuring continuity of operations.

CONTACTS

Omer Tene
Partner

otene@goodwinlaw.com
Boston | +1 617 570 1094

Justin C. Pierce
Partner

jpierce@goodwinlaw.com
Washington, DC | +1 202 346 4006

Federica De Santis
Counsel

fdesantis@goodwinlaw.com
Boston | +1 617 570 1697

Gozde Guckaya
Associate

gguckaya@goodwinlaw.com
Boston | +1 617 305 6778