Updates
January 23, 2025
DOJ’s Final Rule on Data Transfers: Impacts Across Industries

As of January 23, 2025, the regulation discussed below has not been withdrawn by the Trump administration and is not subject to automatic withdrawal under President Trump’s Executive Order freezing regulations. It currently is scheduled to take effect on April 8, 2025. Under the new Trump Executive Order, agencies may postpone implementation of pending regulations for up to 60 days to conduct a policy review.

The U.S. Department of Justice (DOJ) issued its final rule (Final Rule) governing the transfer of government-related data and bulk U.S. person sensitive data to countries of concern, such as Russia, China, and Iran. The rule is not specific to any industry or business and covers data transfers and vendor, employment, and investment agreements that would provide those countries—or businesses or individuals subject to their jurisdiction—with covered data or access to that data. Businesses should assess whether they are engaged in data transactions the rule covers, whether they must change their practices to comply with the rule, and whether and how to implement risk-based compliance programs.

President Joe Biden issued Executive Order (EO) 14117 in February 2024 to mitigate national security risks posed by threat countries’ access to sensitive personal data and government-related data. The EO directed DOJ to issue implementing regulations and directed the U.S. Department of Homeland Security (DHS) to develop related security measures for classes of transactions.

DOJ issued its Final Rule on December 27, 2024. The Final Rule incorporates feedback received on DOJ’s October 2024 Notice of Proposed Rulemaking (NPRM) and March 2024 Advance Notice of Proposed Rulemaking (ANPRM). The NPRM included several notable updates from the ANPRM. The Final Rule largely tracks the NPRM but refines some definitions and adds and modifies some examples. The Final Rule announcement also indicates where DOJ declined to make changes, which further clarifies the focus of the new rule. The Final Rule also added detail about compliance and enforcement regimes, which will be addressed separately.

Overview

The rule is a national security rule, not a privacy rule. Concepts familiar to privacy professionals, such as the consent of a data subject or exemptions for anonymized or aggregated data, are absent from the rule because they do not mitigate the national security threats the government has identified. At a high level, the rule arises from the U.S. government's premise that any foreign company or individual subject to the jurisdiction of a "Country of Concern" (CoC) could be compelled to permit the CoC to leverage access to Americans' data and that the CoC could use the resources of a national intelligence service to exploit that data to the detriment of U.S. national security.

Accordingly, the rule prohibits "data brokerage" transactions that provide CoCs or covered persons (CPs) with government-related data, bulk U.S. person sensitive data (BUSPD), or access to such data. The rule restricts vendor, employment, and investment agreements that would provide such data or access and imposes security requirements to mitigate the threat those agreements present.

The rule does not apply to data transactions between a U.S. person and another U.S. person. It applies only to data transactions in which a U.S. person provides a CoC or CP with covered data or access to covered data and to data brokerage transactions in which a U.S. person provides covered data or access to a *foreign* person who is not a CoC or CP (more on this below).

Although DOJ stated its intent to provide guidance on the due diligence it "expects" U.S. persons to conduct related to data transactions, the rule generally adopts a "knowingly" standard. A U.S. person is only liable for conduct, circumstances, or results that the U.S. person had actual knowledge of or reasonably should have known about. Deliberate avoidance of knowledge will not vitiate liability.

Notable Issues and Changes in the Final Rule

Third-Party Services

The ANPRM and NPRM prompted substantial feedback regarding the responsibilities of U.S. providers of third-party services, such as cable operators and cloud service providers (CSPs) and their U.S. customers. DOJ declined to establish a blanket exemption for third-party providers and instead emphasized that under the "knowingly" standard, a third-party provider is not required to take affirmative steps to discover whether its customers are engaging in transactions subject to the rule.

Onward Transfers

If a U.S. person engages in a data brokerage transaction with a *foreign person* (FP) that is not a CP or CoC, the U.S. person must contractually bind the FP to refrain from engaging in a data brokerage transaction with a CoC or CP involving the same data.

The rule further requires the U.S. person to report any known or suspected violations of the contractual requirement within 14 days, with no exceptions, and sets out requirements for such reporting. DOJ declined to prescribe specific due diligence requirements for compliance, but DOJ stated that "At a minimum . . . U.S. persons must conduct sufficient due diligence to be able to comply with the reporting requirements, which could include periodic reviews with foreign counterparties to ensure that they have complied with the contract." DOJ anticipates providing general compliance guidance, which may include suggested contractual clauses and compliance mechanisms.

Know Your Data

DOJ will expect companies to "know their data" when dealing in government-related data and BUSPD, but that does not impose a requirement to decrypt data.

IP Addresses

The Final Rule notably backs away from the NPRM's proposal to include IP addresses within "precise geolocation data." Instead, IP addresses are "listed identifiers" and are only subject to the Final Rule when combined with other listed identifiers or other information.

Telecommunications Services

DOJ expanded the definition of "telecommunications services" for purposes of scoping an exemption for data transactions ordinarily incident to and part of such services from the Telecommunications Act definition, 47 U.S.C. § 153(53), to include voice data communications regardless of format or mode of delivery, including over cable, IP, wireless, fiber, and other means, as well as "arrangements for" network interconnection, transport, messaging, routing, or international voice, text, and data roaming. Providers of such services will benefit from this exemption in a technology-agnostic way. As noted below, however, DOJ rejected a broader exemption for communications networks.

Personal Financial Data

DOJ's announcement reiterates that the exemption for transfers of personal financial data ordinarily incident to sales applies to sales of all products, such as through online marketplaces, and not just financial services.

Focus on Ads

The NPRM and Final Rule contain several examples involving the sale of online advertising. DOJ remains focused not only on the use of ad IDs as personal data (when combined with other identifiers, such as IP address), but also in the transfer of personal data as part of advertising sales.

Focus on AI

The NPRM and Final Rule contain several examples involving AI models. DOJ remains focused on the idea that AI could disclose its training data, which could constitute a covered transaction if the training data includes data subject to the rule.

Corporate Group Transactions

DOJ clarified in the Final Rule that if a U.S. person company has a subsidiary that is organized under the laws of a CoC or has its principal place of business in a CoC, the subsidiary is a CP. Vendor agreements with the subsidiary would be subject to the rule.

Role of Encryption

Compared to the NPRM, encryption still does not exempt data from the rule. DOJ rejected a proposal to exempt data subject to post-quantum encryption. The Final Rule recognized that encryption is a useful and important tool for facilitating restricted transactions but that encryption cannot be used to exempt data from the rule.

Financial Services Exemption

DOJ clarified the exemption for cybersecurity services. The Final Rule now states that cybersecurity services performed in conjunction with processing payments and fund transfers can be ordinarily incident to and part of provision of covered financial services. On the other hand, product development is not.

Corporate Group Transactions Exemption

Under the Final Rule, the exemption applies to the foreign subsidiary's access to personal financial data ordinarily incident to and part of provision of customer support. The exemption does apply to shared use of centralized risk-monitoring applications used to monitor for fraud but does not apply to a foreign subsidiary's access to U.S. person data for the purpose of providing customer service to U.S. persons. This is also consistent with 202.505(b)(4).

Health Data

The definition of "personal health data" now covers data that "indicates, reveals, or describes" an individual's past, present, or future physical or mental health condition; provision of healthcare to an individual; or payment for the provision of healthcare. Data does *not* have to *identify* an individual to meet this definition. Personal health data is subject to the rule regardless of whether the transacting parties are subject to the Health Insurance Portability and Accountability Act (HIPAA), and health data that is de-identified consistent with HIPAA is *not* excluded or exempted from the rule.

Scientific Research

DOJ made several modifications and clarifications to accommodate international scientific and medical research, for example excluding routine clinical measurements from certain categories of 'omics data. Researchers should seek guidance specific to their particular research projects about the precise application of the exceptions.

Reporting Requirement

A U.S. person that receives and rejects an offer to engage in a prohibited transaction must report it to DOJ within 14 days of rejecting it.

Changes Declined

DOJ rejected numerous proposals. DOJ's rejections further illuminate the government's threat assessment and objectives, which will likely inform enforcement priorities. Examples of proposals DOJ declined to adopt include:

- Exempting anonymized data.
- Exempting encrypted data, including data encrypted to post-quantum encryption standards.
- Exempting aggregated data.
- A consent-based exemption.
- A blanket exemption for third-party providers (relying instead on the "knowingly" standard).
- An exemption for product research, development, or improvement.
- An exemption for data transactions incident to the function of communications networks (DOJ concluded this would functionally exempt IP addresses).
- An exemption for transactions with contractual provisions retaining U.S. persons' direction and control over data processing.
- An exemption for transactions with contractual provisions requiring a CP to maintain privacy and secrecy of information.

- An exception to “onward transfer” liability for *de minimis* transfers, good faith, or inadvertent violations.
- A safe harbor for due diligence practices.

Takeaways for US Businesses

As we previously stated in our Update regarding the NPRM, U.S. businesses should assess whether they expose covered U.S. person or U.S. government-related data to countries of concern or to covered persons. With the Final Rule coming into effect, U.S. businesses should work with legal professionals to assess whether they engage in data transactions that implicate the proposed rule and whether to implement risk-based compliance measures. The Cybersecurity and Infrastructure Security Agency security requirements and DOJ’s compliance and enforcement provisions will be addressed in a separate Update.

Authors

Explore more in

Emerging Companies & Venture Capital Law Privacy & Security White Collar & Investigations

Related insights

Blog

DOJ’s Notice of Proposed Rulemaking on Sensitive Personal Data and Government-Related Data