wiley

ALERT

Action Steps To Address New Restrictions On Outbound Data

May 16, 2024

This article was originally published in Law360 on May 10, 2024 and can be found here.

The U.S. Department of Justice published an advance notice of proposed rulemaking on March 5 that breaks new ground by proposing to restrict data flows out of the U.S. The ANPRM implements a February executive order that directs the DOJ to prevent access to certain U.S. data by countries of concern, such as China.[1]

The **passage into law** of the Protecting Americans' Data from Foreign Adversaries Act, as part of the supplemental appropriations bill, H.R. 815, on April 24, raises similar implementation questions for the Federal Trade Commission.

In the ANPRM, the DOJ proposes to prohibit data brokerage transactions with covered persons — entities or people linked to countries of concern — and put security requirements on restricted data transactions with covered persons incident to employment, vendor or investment agreements.

In addition, because of definitional uncertainties around data brokerage and other key terms, it may require U.S. companies to introduce contract terms for data brokerage transactions, as defined in the regulation, with any foreign entity to prevent onward data transfers to China and other countries of concern.

Many questions on the contours of the regulation remain unanswered, and the DOJ has a lot of work left to do. The agency received dozens

Authors

Greta M. Peisch
Partner
202.719.3378
gpeisch@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Practice Areas

Export Controls and Economic Sanctions
International Trade
Telecom, Media & Technology

of comments on the notice from an array of participants in the digital economy.

Like the ANPRM, the new law prohibits data brokerage transactions with foreign adversary countries, and it is unclear whether its passage will affect the scope of data brokerage restrictions in the ANPRM.

Either way, companies should take steps to understand how the creation of new restrictions on data relates to their operations and take steps to understand their potential compliance risks. Taking the time to understand their risks now will enable firms to consider strategies to mitigate that risk and more effectively participate in future steps in the rulemaking process.

Initial Steps

An initial assessment of risk should include the following factors.

Know your data.

As a threshold matter, companies need to understand whether their data includes covered personal identifiers, and, if so, how much of it their datasets include.

The proposed rule would cover specific listed identifiers, ranging from Social Security numbers to geolocation data to advertising identifiers, that are "reasonably linked to an individual." Restrictions on transfer kick in if the amount of data hits certain thresholds over a 12-month period.

Companies should also determine whether they hold government-related data, which would be subject to stricter requirements.

Know your data-based internal operations.

Even before evaluating arm's-length transfers of data, companies must understand their internal uses and treatment of data. Although the ANPRM contemplates a narrow exemption for intra-entity transactions, the exemption as written is limited in scope, and may not cover data transfers and uses related to core business practices.

Companies with employees or subsidiaries in potential countries of concern should evaluate whether their internal use of data presents risks.

In addition, processes that may be considered internal could involve an outside vendor, such as payroll, human resources management, collaboration software, etc. Companies will need to understand whether these internal functions involve outside access to data and how.

Know whether counterparties to your data transactions are covered persons.

Companies will need to evaluate their external data transaction counterparties and vendors. The transactions subject to the regulation are broad, and any commercial transaction or relationship involving bulk U.S. sensitive data is subject to the ANPRM.

A review of repeat or potential counterparties and their connections to countries of concern will help identify risks in a company's business model. Companies should evaluate, to the extent possible, whether counterparties — or entities in their corporate family — are organized under a country of concern's laws, are more than 50% owned by a country of concern or have business operations or employees in a country of concern.

Develop compliant contractual terms.

The ANPRM proposes contractual requirements for data brokerage transactions with any foreign parties to prohibit the onward transfer of U.S. bulk sensitive personal data or government-related data to countries of concern.

Although the explicit contractual term only applies to data brokerage transactions with foreign parties, companies may want to consider applying contractual terms to other categories of transactions to mitigate the risk of falling afoul of the regulations.

Review current data security measures.

Certain transactions — classified as vendor agreements, employment agreements and investment agreements — in which the counterparty to the transaction is a covered person may be permitted, if certain data security requirements are met. Companies should evaluate their current security measures and potential steps they would need to take to meet the types of requirements that may be imposed in a final rule.

Evaluate licensing, interpretative guidance and compliance programs.

The DOJ is contemplating creating a licensing program similar to that of the Office of Foreign Assets Control. This would be a major change in how data is regulated, establishing a permission-based approach to exporting data beyond the U.S. As export control teams know, a licensing process can introduce delay and uncertainty in international transactions.

The DOJ is also contemplating whether it should provide interpretive guidance, and suggests that it will take an enforcement approach that emphasizes risk-based compliance programs.

Based on assessments of data uses and transactions, companies should evaluate the need for licenses to

cover certain activities or for clarification on the application of the regulations.

Conclusion

Companies should contemplate what a risk-based compliance program will look like based on the types of data and transactions involved.

This regulatory activity by the DOJ is just one of several major moves happening in U.S. policy affecting data governance and transfers. The implementation of new restrictions on the movement of data has the potential to significantly affect any company that collects or handles data linked to individuals. The first step in understanding the impact is to assess all data-based operations. Companies should track these issues and, as appropriate, participate in policy development.

***

This regulatory activity by the DOJ is just one of several major moves happening in U.S. policy affecting data governance and transfers. The implementation of new restrictions on the movement of data has the potential to significantly affect any company that collects or handles data linked to individuals. The first step in understanding the impact is to assess all data-based operations. Wiley's team has been advising clients and industries on U.S. and global data regulations and the overlap of growing security justifications for domestic regulations. Our Privacy, Cyber & Data Governance practice teams with our International Trade and Export Control teams to stay ahead of regulatory risk. We urge our clients to track these issues and, as appropriate, participate in policy development.

[1] The DOJ has proposed using the definition of "countries of concern" created by the U.S. Department of Commerce. The ANPRM stated that it is considering the following as countries of concern: People's Republic of China, along with the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau; the Russian Federation; the Islamic Republic of Iran; the Democratic People's Republic of Korea; the Republic of Cuba; and the Bolivarian Republic of Venezuela.