Milbank

Insights

Global Risk & National Security Practice

U.S. Executive Order Proposes Restrictions on Certain Cross-Border Data Transactions

March 4, 2024

Contacts

John M. Beahn, Partner
+1 202.835.7520
jbeahn@milbank.com

Dara A. Panahy, Partner
+1 202.835.7521
dpanahy@milbank.com

Bijan Ganji, Partner
+1 202.835.7543
bganji@milbank.com

Nola B. Heller, Partner
+1 212.530.5108
nheller@milbank.com

Nicholas A. Smith, Partner
+1 202.835.7522
nsmith@milbank.com

Matthew Laroche, Partner
+1 212.530.5514
mlaroche@milbank.com

Tawfiq S. Rangwala, Partner
+1 212.530.5587
trangwala@milbank.com

Dana Zelman, Special Counsel
+1 202.835.7523
dzelman@milbank.com

Lafayette M. Greenfield, Special Counsel
+1 202.835.7512
lgreenfield@milbank.com

On February 28, 2024, the Biden Administration released an Executive Order ("EO") that will establish new regulations prohibiting, or otherwise restricting, certain categories of commercial data transactions that pose an unacceptable risk to U.S. national security. In issuing the EO, the Biden Administration concluded that U.S. adversaries are "exploiting Americans' sensitive personal data to threaten our national security" and thus new regulations are necessary to prevent the purchase or access to such data by countries that may use it for nefarious purposes.

As described more fully below, the proposed regulations focus on prohibiting and restricting specified categories of commercial transactions involving the purchase or acquisition of bulk U.S. sensitive personal data or any U.S. government-related data, by individuals or entities located in certain countries. The proposed regulations identify six (6) "countries of concern" subject to the regulations: China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela. The EO directs the U.S. Department of Justice ("DOJ") to promulgate the regulations, in consultation with the U.S. Departments of State, Commerce, Treasury, and Homeland Security. DOJ issued an accompanying Advanced Notice of Proposed Rulemaking ("ANPRM") that includes details on the proposed regulations and commences a lengthy regulatory process to finalize the regulations. The EO does not prescribe a date by which the regulations must be implemented, though initial comments on the ANPRM are due 45 days after its publication in the U.S. Federal Register, which is scheduled for March 5, 2024 (available here).

The proposed regulations build on other tools that the U.S. government has deployed to secure and protect sensitive personal data of U.S. persons, including case-by-case reviews of inbound foreign investments by the Committee on Foreign Investment in the United States. It also effectively creates a new data security regulatory regime that could have broad implications for domestic and international businesses, especially those that maintain or collect large amounts of personal data of U.S. persons and U.S. government entities. These businesses will be subject to new regulations that could impact existing

or future business operations or revenue streams and also add compliance costs and burdens. Impacted business thus should closely review DOJ's rulemaking proceeding to understand any potential impacts.

Key highlights from the EO and ANPRM include the following:

Covered Data Transactions

The ANPRM defines the types of data transactions subject to the proposed regulations as "covered data transactions." Under the proposed regulations, a covered data transaction includes "any transaction that involves any bulk U.S. sensitive personal data or government-related data and that involves (1) data brokerage; (2) a vendor agreement; (3) an employment agreement; or (4) an investment agreement." The ANPRM broadly defines a "transaction" subject to the regulations as any that involves the "acquisition, holding, use, transfer, transportation, exportation of, or dealing in" the relevant data.

The ANPRM determines that two types of covered data transactions will be prohibited outright. These include transactions with a country of concern involving "data brokerage" (the sale or licensing of bulk U.S. sensitive personal data or government-related data) or "genomic data" (the transfer of bulk human genomic data or biospecimens from which such data can be derived). The ANPRM also classifies certain covered data transactions that will be restricted and permitted only if they comply with predetermined security requirements to mitigate access to sensitive personal data by entities located in countries of concern. These include (i) vendor agreements for the provision of goods and services (including cloud-service agreements); (ii) employment agreements; and (iii) investment agreements. Transactions of these types with individuals or entities located in countries of concern will be permitted only if they comply with security requirements that the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency will establish.

The ANPRM proposes several across-the-board exemptions for commercial data transactions that will be exempt from the forthcoming regulations. These include commercial data transactions that are (i) ordinarily incident to and part of "financial services, payment processing and regulatory compliance" activities such as banking, capital markets or financial-insurance activities; (ii) ordinarily incident to and part of "ancillary business operations" such as payroll and human resources; and (iii) required or authorized by federal law.

Bulk U.S. Sensitive Personal Data and U.S. Government-related Data

As noted above, a covered data transaction must involve "bulk U.S. sensitive personal data" or "U.S. government-related data." The ANPRM classifies U.S. sensitive personal data into six broad categories: (i) personal identifier information, (ii) personal financial data; (iii) precise geolocation data, (iv) biometric identifiers, (v) human genomic data; and (vi) personal health data. Depending on the sensitivity of the categories of sensitive personal data involved, the ANPRM proposes a broad range of the number of records that would constitute "bulk" for purposes of the regulations (anywhere from 100--1,000,000 U.S. person records). This broad definition means that transactions involving data on relatively small numbers of U.S. persons could be subject to the regulations.

The ANPRM further proposes to define "U.S. Government-related data" to include two categories of data: precise geolocation data and *any* sensitive personal data that can be linked to current or former employees or contractors of the U.S. government or military. Importantly, U.S. government-related data would be in-scope for the regulations regardless of its volume—meaning that any number of records could trigger the regulations.

Countries of Concern

As noted above, the DOJ ANPRM proposes the following six countries of concern: China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela. At this time, it is unclear whether

additional countries will be added to the list going forward, and what the requirements will be for another foreign state to be included in the future.

Covered Persons

Importantly, the regulations only will apply to the extent that a covered data transaction involves an individual or entity located in, or subject to the jurisdiction, of a country of concern. The EO refers to such individuals or entities as "covered persons" and identifies four specific categories of covered persons: (i) an entity majority owned or controlled by, or otherwise subject to the jurisdiction of, a country of concern; (ii) a foreign person who is an employee or contractor of such entity; (iii) a foreign person who is an employee or contractor of the government of a country of concern; or (iv) a foreign person who is "primarily resident" in the territory of a country of concern.

Application and Enforcement

DOJ noted in the ANPRM that it is not intending to impose due diligence or other affirmative recordkeeping or reporting requirements on U.S. businesses in connection with the regulations. Instead, DOJ stated that it expects businesses to adopt internal compliance programs to implement the regulations similar to programs businesses have adopted to comply with the economic sanctions-based programs administered by the U.S. Department of Treasury's Office of Foreign Assets Control. If a violation of the regulations were to occur, DOJ indicated that it would consider the adequacy of an internal compliance program in any enforcement action. With that said, failure to comply with the requirements of the program could subject U.S. businesses and investors to criminal and civil penalties. DOJ stated that it is considering establishing specific civil penalties for violations of the regulations during its regulatory proceeding. Finally, while the new regulations will apply prospectively, the EO directs DOJ and the other agency heads to recommend actions to detect, assess and mitigate prior transfers of bulk sensitive personal data to countries of concern. Businesses will need to closely monitor these recommendations to determine whether they could have any impact on prior business activities.

Key Takeaways

The clear focus of the proposed regulations is to prohibit and restrict the sale or brokerage of large amounts of U.S. sensitive personal data to China and other countries of concern. The EO specifically notes that the new regulations will not impose generalized data localization requirements or broadly require that computer processing facilities be located in the United States, but the regulations could apply to other contexts. These include offshore access by third parties or affiliated entities to U.S. customer records, transfers of U.S. business records to overseas business partners and collaborative research and development activities. The proposed regulations thus could have broad implications on domestic and international businesses, which could be subject to regulations that impact existing or future business operations or revenue streams. Impacted business thus should closely review DOJ's rulemaking proceeding to understand any potential impacts.

* * * *

Practice/Group Contacts

Washington, DC	1850 K Street, NW, Suite 1100, Washington, D.C. 20006
New York	55 Hudson Yards, New York, New York 10001

John M. Beahn	jbeahn@milbank.com	+1 202.835.7520
Dara A. Panahy	dpanahy@milbank.com	+1 202.835.7521
Bijan Ganji	bganji@milbank.com	+1 202.835.7543
Nola B. Heller	nheller@milbank.com	+1 212.530.5108
Nicholas A. Smith	nsmith@milbank.com	+1 202.835.7522
Matthew Laroche	mlaroche@milbank.com	+1 212.530.5514
Tawfiq S. Rangwala	trangwala@milbank.com	+1 212.530.5587
Dana Zelman	dzelman@milbank.com	+1 202.835.7523
Lafayette M. Greenfield	lgreenfield@milbank.com	+1 202.835.7512

Please feel free to discuss any aspects of this Client Alert with your regular Milbank contacts or any member of our Global Risk & National Security and Cybersecurity teams.