Skadden

Cybersecurity and Data Privacy Update

March 6, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., N.W.
Washington, D.C. 20005
202.371.7000

A Fracturing Data Environment: Executive Order Portends Major Changes to US Data Management

Takeaways

- The Biden administration, led by the Department of Justice (DOJ), is considering establishing a regulatory regime that would prohibit or restrict the bulk transfer of U.S. personal data and certain U.S. government data to covered persons or countries of concern (COC), which currently include China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and Venezuela.
- The U.S. government seeks to establish categories of prohibited or restricted transactions supplemented by list-based individual and entity designations.
- Purely U.S.-to-U.S. transactions appear exempt, but it is unclear how the proposed rule will impact intracompany arrangements not otherwise explicitly exempt.
- Companies will be required to implement policies and procedures to comply with the new rules rather than seek a case-by-case review by the U.S. government.
- The DOJ is considering a licensing regime to provide case-by-case exemptions or classes of exemptions through general and specific licenses as well as providing parties an opportunity to seek advisory opinions in consultation with the Department of State, the Department of Commerce and the Department of Homeland Security.
- Proposed regulations are due within 180 days of the publication of Executive Order 14117 — expected to occur by mid-March 2024 — and compliance will not be required until a final rule is issued.
- Penalties for failure to comply are still under consideration and will likely include civil remedies available under the International Emergency Economic Powers Act (IEEPA).

Background

On February 28, 2024, President Biden issued Executive Order 14117 (the EO) on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" that would regulate the transfer of bulk U.S. persons' data and certain U.S. government data to countries of concern. Concurrently, the DOJ released an Advance Notice of Proposed Rulemaking (ANPRM; the ANPRM and EO together as the proposal), which outlines a proposed regulatory regime to implement the EO. This order builds upon prior executive orders regulating (i) information and communications technology and services (ICTS) (including connected software applications) from countries of concern and (ii) the use of U.S. cloud services by countries and persons of concern.

A Fracturing Data Environment: Executive Order Portends Major Changes to US Data Management

Overview

The proposal seeks to prohibit and restrict "covered data transactions" between "U.S. persons" and "covered countries of concern" or "covered persons" that involve the transfer of "bulk U.S. sensitive personal data" or "government related data." The new regime will not impose generalized data or computing facility localization requirements nor a case-by-case review of transactions. Industry will rather be expected to comply with applicable transaction restrictions and will likely face civil monetary penalties for noncompliance.

COCs and Covered Persons

COCs are defined to include China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and Venezuela. The DOJ has indicated that covered persons will include (i) companies owned by, controlled by or subject to the jurisdiction or direction of a country of concern; (ii) foreign employees of, or contractors with, such entities or a COC; and (iii) foreign persons who are primarily residents of a COC. The attorney general will be able to supplement these definitions by designating any persons found to be enabling circumvention as covered persons.

The proposal seeks to exempt U.S. persons from these categories of covered persons. U.S. persons will include U.S. citizens, wherever located, and individuals, including nationals from COCs, who are legally resident or located in the United States.

Sensitive Personal Data

The proposal identifies six categories of non-public "sensitive personal data," including anonymized, pseudonymized, de-identified or encrypted data, subject to bulk thresholds ranging from one hundred to one million as "bulk U.S. data":

1. specifically listed categories and combinations of covered personal identifiers (not all personally identifiable information);
2. geolocation and related sensor data;
3. biometric identifiers;
4. human genomic data;
5. personal health data; and
6. personal financial data.

The proposal seeks to exclude expressive content (*e.g.*, videos, artwork and publications), but it will include data collected on employees unless otherwise exempt. Prohibitions will also depend upon key characteristics of the data, such as whether it is limited to commercial data and whether it concerns particular categories of individuals — such as journalists, NGOs or political figures.

The proposal also seeks to establish controls over U.S. government-related data, for which there is no bulk threshold. U.S. government-related data includes geolocation data related to certain facilities and sensitive personal data of U.S. government employees.

Covered Data Transaction

The ANPRM defines a "transaction" broadly to include "any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest." A "covered data transaction," however, is defined more narrowly as a 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."

Prohibited covered data transactions include all data brokerage transactions and bulk genomic-data transactions. Restricted covered data transactions would include vendor, employment and investment agreements. Restricted covered data transactions are otherwise permitted if certain security measures are implemented as outlined in the ANPRM, including (i) implementing basic organizational cybersecurity posture requirements; (ii) performing data minimization and masking, using privacy-preserving technologies, developing information-technology systems to prevent unauthorized disclosure, implementing logical and physical access controls and (iii) ensuring independent auditing. The ANPRM further describes these covered transactions as follows:

1. **Data brokerage** would include the sale of, licensing of, access to or similar commercial transactions involving the transfer of bulk U.S. sensitive personal data or U.S. government-related data to include providing a covered person access to such data.
2. **Vendor agreements** would include agreements or arrangements (to include services related to the provision or use of cloud computing, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)) that allow a covered person to process, store or access bulk U.S. sensitive personal data or U.S. government-related data.
3. **Employment agreements** would include employment arrangements — including with executive officers and board members — involving persons located in China or otherwise designated by the attorney general as a covered person for roles involving access to bulk U.S. sensitive personal data or U.S. government-related data.

4. **Investment agreements** would include active investments in (1) real estate located in the United States or (2) a U.S. legal entity such as a data center or business that systematically collects bulk U.S. sensitive personal data of its U.S. users. Investment agreements would not include pre-commercial companies or startup companies that do not yet maintain or have access to bulk U.S. sensitive personal data or U.S. government-related data or purely passive investments.

Importantly, the ANPRM further seeks to prohibit U.S. persons from "knowingly" directing transactions that would be prohibited if engaged in by a U.S. person, similar to concepts adopted in the proposed semiconductor export rules and outbound investment regime.

1. The ANPRM articulates a number of important exceptions, including transactions:
2. incident to financial services transactions for banks and financial institutions including e-commerce;
3. for the conduct of the official business of the U.S. government;
4. involving personal communications or informational materials;
5. required or authorized under federal law or international agreements; or
6. involving intra-entity transactions incident to business operations (*e.g.*, human resources).

Application and Enforcement

The DOJ will administer the regime with consultation from the Department of State, the Department of Commerce and the Department of Homeland Security. The proposal requires industry to undertake risk-based compliance, affirmative diligence and recordkeeping. The DOJ anticipates imposing civil monetary penalties for noncompliance as is the case with analogous regulatory regimes, including certain sanctions and export control contexts. Company internal compliance policies will be scrutinized as part of any assessment for penalties. Companies will be able to seek license exceptions and advisory opinions. Being authorized under IEEPA, the regime can be expected to prohibit evasions, causing violations, attempts and conspiracies. The DOJ is also considering IEEPA-based reporting requirements.

Relationship With Other Authorities

The EO requires that the DOJ coordinate with other U.S. government departments and agencies, including the Department of Commerce (ICTS) and the Committee on Foreign Investment in the United States (CFIUS), although the DOJ does not intend that the proposal will have a significant overlap with existing authorities. For example, with respect to investment agreement that are also CFIUS covered transactions, the DOJ expects to regulate covered data transactions that are investment agreements unless CFIUS enters into and imposes mitigation measures to resolve national security risk. In the latter case, parties to a covered investment agreement would not be able to seek a license under the proposal and CFIUS would otherwise be able to impose additional mitigation measures on top of an investment agreement needed to address national security risks. The proposal would otherwise regulate covered data transactions that go beyond CFIUS's jurisdiction to include those investment agreements that are not CFIUS covered transactions, risks associated with CFIUS covered transactions that do not arise as a result of the transaction and risks that may arise in the temporal gap between entering into an investment agreement but before submitting a CFIUS filing.

Commercial Considerations

The proposal seeks to streamline what was once a bespoke patchwork of mitigation measures imposed by CFIUS in the absence of comprehensive data privacy legislation and targets only a specific class of transactions considered the highest national security risks. Data brokers are a primary target of the new restrictions, and we anticipate that the EO will have the greatest impact on companies that operate in this space. However, by repurposing familiar regulatory instruments — such as components of existing sanctions or export control licensing regime —with regularly imposed CFIUS mitigation measures to protect access to U.S. bulk personal data, the proposal is bound to engender regulatory uncertainty. Companies can help prepare themselves for the rollout of this new regulatory framework by closely following the rulemaking process and assessing their existing employee, vendor and investment agreements for access to bulk sensitive U.S. data.

A Fracturing Data Environment: Executive Order Portends Major Changes to US Data Management

Contacts

Michael Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

David Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Joshua Silverstein
Counsel / Washington, D.C.
202.371.7148
joshua.silverstein@skadden.com

Tatiana Sullivan
Counsel / Washington, D.C.
202.371.7063
tatiana.sullivan@skadden.com

Alyssa Domino
Associate / Washington, D.C.
202.371.7139
alyssa.domino@skadden.com

Nicholas Kimbrell
Associate / Washington, D.C.
202.371.7337
nicholas.kimbrell@skadden.com