PRESIDENT BIDEN ISSUES EXECUTIVE ORDER RESTRICTING BULK TRANSFERS OF SENSITIVE PERSONAL AND US GOVERNMENT-RELATED DATA

Date: 21 March 2024

US Policy and Regulatory Alert

By: Jake Bernstein, Guillermo S. Christensen, David C. Rybicki

On 28 February 2024, President Biden issued Executive Order 14117 of February 28, 2024, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern (EO) aimed at restricting bulk transfers of certain sensitive data outside the United States to certain foreign parties and establishing security guidelines for sensitive data stored in the United States. The EO represents a broad new initiative to restrict large-scale transfers of personal data to foreign entities, an area that has largely been unregulated, and is generally aligned with a series of administrative actions aimed at protecting the sensitive personal data of US citizens and military personnel. This new initiative is also separate and distinct from data privacy laws, whether federal or state, although some of the types of data covered by the EO are also subject to data protection laws for other reasons. To underscore the Biden administration's focus, Matt Olsen, the assistant attorney general (AAG) for the National Security Division of the Department of Justice (DOJ), subsequently publicly cautioned companies on 8 March that they need to develop a more comprehensive understanding of the nature of the data they collect, store, and process. AAG Olsen also recommended that companies review and update data-sharing agreements, ahead of implementation of the EO's provisions.

The EO is designed to restrict the ability of foreign adversaries to access and use sensitive personal data of US citizens and data associated with US government-related activities and is part of a broader effort by the US government to address a range of concerns around the export of technology, services, and data.

Shortly before this EO was announced, the Department of Commerce published a proposed rule, Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities (Proposed Rule), to begin implementing novel requirements on Infrastructure-as-a-Service (IaaS)[1] providers and their US and foreign resellers. If the proposed rule is implemented, it would impose significant “know your customer” and reporting requirements on cloud computing service providers engaging in foreign business and subject them to penalties for noncompliance.[2]

In explaining its rationale for issuing the EO, the White House highlighted recent efforts by foreign adversaries to acquire sensitive data through legal means and exploit the data to engage in blackmail, scams, surveillance, and other illegal behavior. For example, the administration explained that sensitive data can be used to surveil foreign dissidents in the United States or journalists that report on international affairs. The White House also stressed the need to protect members of the military and other national security personnel, whose personal data may be used by foreign adversaries to blackmail them or track activity, potentially compromising US national security.

©2005-2026 K&L Gates LLP. All Rights Reserved.

Although not discussed explicitly, another motivation is driven by analysis in the intelligence community on the value of so-called commercially available information for broader economic and technical purposes, such as large data sets for machine learning and AI, or for analysis of economic trends.[3] The EO does not impose any immediate obligations on US or foreign entities but instead directs the DOJ, Cybersecurity Infrastructure Security Agency (CISA), and Department of Homeland Security (DHS) to promulgate regulations implementing these goals. We expect significant input from a wide range of stakeholders during the comment period.

The EO directs agencies to undertake three categories of regulatory activity:

First, the EO directs the DOJ and DHS to issue regulations that would prohibit or restrict certain transfers of bulk sensitive personal data and US government-related data to “foreign countries of concern” and “covered persons.” The DOJ already initiated rulemaking proceedings to clarify the scope of these terms and the forthcoming restrictions, as described further below. The EO separately directs CISA and the DOJ to publish security requirements for protection of bulk sensitive personal data based on the Cybersecurity and Privacy Frameworks developed by the National Institute for Standards and Technology. CISA and the DOJ are further directed to develop interpretive and enforcement guidance to uphold the security requirements.

Second, the EO also requires that the DOJ's Committee for Foreign Participation in the United States Telecommunications Services Sector review licenses for submarine cable systems owned or controlled by, or that terminate in, “foreign countries of concern” and to issue policy guidance regarding its reviews of license applications and existing licenses.
Third, the EO directs a mix of federal agencies to review existing government contracts and grants to ensure that foreign countries of concern are not able to access health and genomic data through existing programs. It also directs the DOJ, DHS, and the director of national intelligence to evaluate risks posed by prior transfers of data to foreign countries of concern.

In conjunction with the White House's publication of the EO, the DOJ released an Advanced Notice of Proposed Rulemaking (ANPRM) to begin the rulemaking process commanded by the EO. The ANPRM aims to more comprehensively address two key questions left open in the EO: (1) to which entities are certain data transfers prohibited and (2) what types of data may not be transferred to foreign entities. Commercial entities that may be subject to the EO should carefully consider the proposed approach outlined in the ANPRM and consider commenting on the efficacy and impact to their operations.

The EO prohibits transfers of certain data to “foreign countries of concern” and “covered persons.” The ANPRM proposes to define “foreign countries of concern” to include six countries: China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela. Additionally, the ANPRM defines “covered persons” as “certain classes of entities and individuals subject to the jurisdiction, direction, ownership, or control of countries of concern because, as a legal and practical matter, providing data to these persons will place that data within the reach of the countries of concern.” The DOJ's proposed definition of “covered persons” is particularly broad and includes “any person resident in a foreign country of concern.” Thus, any transfer of bulk sensitive personal data or US government-related data to a person resident in a country of concern could be a prohibited or restricted transaction under these new regulations.

The ANPRM also proposes definitions for three terms used in the EO that define the scope of data that would be covered by the restrictions. “Sensitive personal data” is defined to include the following categories of data:

©2005-2026 K&L Gates LLP. All Rights Reserved.

1. Specifically listed categories of information;
2. Geolocation data;
3. Biometric identifiers;
4. Human genomic data;[4]
5. Personal health data; and
6. Personal financial data.

Regulations will, however, only cover transfers of "bulk" sensitive personal data and the ANPRM proposed that "bulk" be defined as involving a threshold number of US persons or US devices. The "bulk" limitation will not apply, however, to "US government-related data," which the ANPRM defines as sensitive personal data linked or linkable to current or recent former employees of contractors or the federal government. Finally, the ANPRM further defines the scope of transactions covered by the EO and distinguishes between "prohibited" transactions, which will not be allowed to proceed, and "restricted" transactions, which will be allowed to proceed with a notification to the US government. The ANPRM proposed to define prohibited data transactions as (1) data-brokerage transactions, and (2) certain genomic-data transactions. The ANPRM defines restricted data transactions as (1) vendor agreements involving the provision of goods and services, (2) employment agreements, and (3) investment agreements.

Certain transactions are expected to be exempt from the regulatory prohibitions on data transfers, such as transactions ordinarily incident to and part of financial services, payment processing, and regulatory compliance; transactions incident to and part of ancillary business operations within multinational US companies (e.g. payroll services); certain US government activities; and certain investments that do not convey the rights or influence that ordinarily pose an unacceptable national-security risk with respect to sensitive personal data.

The DOJ is accepting comments on the ANPRM until 19 April 2024. Our team can assist clients in shaping their comments to the ANPRM to ensure most effective presentations of views. Our team of national security, international trade, and government enforcement lawyers and professionals can also begin assisting clients now with early assessments of the potential impact of these restrictions on current and future business operations and plans. We strongly recommend that companies take a holistic view of the impact of restrictions on the transfer of data, technology, and services and include these assessments in their overall compliance and business planning process.

FOOTNOTES

[1] IaaS is typically defined as a cloud computing service that offers computing capability on demand.

[2] The proposed rule is aimed at implementing EO 14110 (entitled Safe, Secure, and Trustworthy Development and Use of AI) and the January 2021-issued EO 13984 (with the same title as the Proposed Rule). The IaaS concern is driven in part by the reported use of US infrastructure by cyber threat actors, to better conceal their activities, and separate concerns about the availability of US infrastructure to power foreign adversaries' development of large language models and other types of Artificial Intelligence (AI), which are otherwise being restricted through export controls on chips and hardware.

©2005-2026 K&L Gates LLP. All Rights Reserved.

[3] ODNI-Declassified-Report-on-CAI-January2022.pdf

[4] The EO describes a new category of “human 'omic” data that includes a broad range of genomic and other data that is essentially locked to the individual.

KEY CONTACTS



JAKE BERNSTEIN
GLOBAL AI AND INNOVATION PARTNER

SEATTLE
+1.206.370.7608
JAKE.BERNSTEIN@KLGATES.COM



GUILLERMO S. CHRISTENSEN
PARTNER

WASHINGTON, DC
+1.202.778.9095
GUILLERMO.CHRISTENSEN@KLGATES.COM



DAVID C. RYBICKI
PARTNER

WASHINGTON, DC
+1.202.778.9370
DAVID.RYBICKI@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.