KIRKLAND & ELLIS

Kirkland Alert

An Unacceptable Risk: Groundbreaking Executive Order Restricts Outbound Transfers of U.S. Personal Data and Government-Related Data to Countries of Concern

05 March 2024

On February 28, 2024, President Biden issued a much-anticipated, first-of-its-kind Executive Order (the "EO"[1]) aimed at protecting U.S. sensitive personal data and U.S. government-related data from exploitation by countries with an established record of collecting and using such data to enable cyber operations, surveillance, scams, blackmail and other malicious activities. The White House remarks[2] on the EO highlight the administration's dual policy goals to balance efforts on maintaining an open internet and trusted, free flow of information while protecting security, privacy and human rights. The EO directs U.S. government stakeholders to draft regulations and policy guidance to implement these objectives.

The Department of Justice ("the DOJ"), as the lead implementing agency for a significant portion of the EO, published an unofficial draft of the Advanced Notice of Proposed Rulemaking (the "Proposed Rules"). The DOJ hopes to accomplish the EO's balanced policy goals through regulations that are simultaneously targeted and comprehensive. However, stakeholders are likely to be on high alert for unintended consequences of the Proposed Rules, including consequences related to who is covered by the rules and the type of data that is scoped into the rulemaking, as we discuss further below. While neither the EO nor the Proposed Rules impose immediate restrictions or requirements on industry, they lay the groundwork for important developments and forecast requirements that some companies may begin preparing for now. Following brief historical context for the EO, we provide an overview of key rulemaking provisions and select takeaways further below.

Historical Context for National Security Response to Data Threats

The EO is an expansion of a 2021 Executive Order by the same number, which was issued to help secure the U.S. information and communications technology and services supply chain.[3] This updated and expanded EO follows years of increasing U.S. government emphasis on access to data, a concern that has bipartisan Congressional support and which has received policy attention from both the Trump and Biden administrations.[4] Although this EO draws on regulatory concepts familiar to the U.S. Departments of Commerce and Treasury (e.g., general and specific licenses, a specially designated list, and advisory opinions), it places the DOJ in the lead, evincing a potential intent to focus more on enforcement.

The DOJ's particular leadership role in addressing data-security risk includes its review of foreign participation in the U.S. telecommunication sector[5] and its review of foreign investments as a member of the Committee on Foreign Investment in the United States ("CFIUS"). As a frequent co-lead agency reviewing CFIUS transactions, the DOJ has rigorously scrutinized transactions involving sensitive personal data and government-related data. They have also led mitigation efforts with respect to foreign investments in data companies by restricting the use of the companies' third-party vendors, requiring enhanced data privacy and cybersecurity compliance measures, restricting investor access to data, and imposing related reporting and compliance obligations. The DOJ views the EO as complementing and building upon its particular authorities while also expanding them to address a broader gap in existing national security authorities. As Deputy Attorney General Lisa Monaco stated in remarks on the EO: "The Justice Department has long focused on preventing threat actors from stealing data through the proverbial back door. This executive order shuts the front door by denying countries of concern access to American's most sensitive personal data."[6]

The EO's Direction to Promulgate Regulations

The EO directs certain government stakeholders to take lead roles developing policies and rulemaking across several functional areas:

- **Prohibited and Restricted Data Transactions.** The EO directs the DOJ to, within 180 days, draft regulations to prohibit or restrict certain transactions (each a

"covered data transaction") with entities or individuals subject to the jurisdiction, direction, ownership or control of a "country of concern" ("covered persons") by prohibiting or restricting activities likely to provide these countries with access to covered data – currently, countries of concern are: China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and Venezuela. The regulations, discussed in greater detail further below, will apply to transactions that give "covered persons" and "countries of concern" access to U.S. persons' bulk sensitive personal data or U.S. government-related data.

- **Healthcare Data.** The EO directs the Departments of Health and Human Services, Defense and Veterans, who review federal contracts relating to health data, to take additional steps to protect U.S. person sensitive health data and human genomic data from threats posed directly and indirectly by countries of concern. These steps include issuing regulations — pursuant to the agencies' federal contracting oversight — to prohibit or place conditions on contracts, awards and grants that could enable access by countries of concern to such data.
- **International Data Transmission.** The EO directs the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector ("Team Telecom", which the DOJ chairs), to: (i) prioritize its reviews of existing licenses for submarine cable systems that implicate a country of concern (systems owned or operated by persons owned by, controlled by or subject to the jurisdiction or direction of a country of concern, or that terminate in the jurisdiction of a country of concern), (ii) issue new policy guidance for the review of new and existing licenses, and (iii) assess the risk — including third-party risk — of data access by countries of concern on a go-forward basis.
- **Illicit Data Broker Sales.** The EO directs the Consumer Financial Protection Bureau to take steps consistent with existing legal authorities to address threats from the data brokerage industry and to enhance compliance with federal consumer protection law.
- **Completed Transfers.** The EO directs the U.S. Attorney General, the Secretary of Homeland Security and the Director of National Intelligence to make recommendations to detect, assess and mitigate national security concerns from previously completed data transfers within 120 days, and to draft regulations addressing the risks within 150 days.

DOJ's Proposed Rules

The Proposed Rules are not immediately effective and will be subject to additional public review and comment. Comments will be due 45 days after the official version of the Proposed Rules is published in the Federal Register. Following a review of public

comments, and potential additional review and comment periods, the DOJ will issue final rules. The rulemaking process is notoriously lengthy, as a general matter, but final rules could be issued as early as later this year. The DOJ's Proposed Rules contain the following key provisions that relate to prohibiting or restricting covered transactions:

- Covered Persons. The Proposed Rules define "covered persons" as those entities or individuals subject to the jurisdiction, direction, ownership or control of countries of concern, i.e., China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and Venezuela ("covered persons"). More specifically, the following would be covered persons:

    1. *An entity that is 50% or more owned, directly or indirectly, by a country of concern, or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern;*
    2. *An entity that is 50% or more owned, directly or indirectly, by an entity described in category (1) or a person described in category (3), (4) or (5);*
    3. *A foreign person who is an employee or contractor of a country of concern or of an entity described in categories (1), (2) or (5);*
    4. *A foreign person who is primarily resident in the territorial jurisdiction of a country of concern; or*
    5. *Any person designated by the Attorney General as being owned or controlled by or subject to the jurisdiction or direction of a country of concern, or as acting on behalf of or purporting to act on behalf of a country of concern or covered person, or knowingly causing or directing a violation of these regulations.*

    The DOJ provides further clarification of the above with its definitions for "U.S. Person" and "foreign person". U.S. person individuals would not be deemed covered persons and would include U.S. citizens, nationals (including dual citizens), lawful permanent residents, refugees and asylees, and individuals who are "in the United States". In contrast, entities that are legally organized or formed solely in the United States would be considered U.S. persons, but potentially could also be deemed covered persons on the basis of their ownership and/or control. Both individuals and entities could be deemed covered persons on the basis of being specially designated under part (5) in a sanctions-style list that the DOJ would maintain.

- **Covered Data.** The EO directs the DOJ to regulate (i) bulk volumes of sensitive personal data of U.S. persons, (ii) sensitive personal data "linked or linkable" to U.S. government personnel (e.g., personal data from a data broker that is marketed as

linked to current or recent former government employees), and (iii) geolocation data that is linked to sensitive government facilities. As contemplated by the Proposed Rules, there are six categories of sensitive personal data: (1) certain personally identifiable data (not currently contemplated to include certain basic demographic/contact data or network-based identifier and account-authentication data); (2) precise geolocation data; (3) biometrics identifiers; (4) human genomic data; (5) personal health data; and (6) personal financial data.

The DOJ is considering using a risk-based approach to assess and assign a specific threshold for "bulk" volume for each category of sensitive personal data (e.g., bulk human genomic data could comprise data of as few as 100 U.S. persons, while personal financial data could comprise data of greater than 1,000,000 U.S. persons). Sensitive personal data will not include data that is a matter of public record.

- **Classes of Prohibited Transactions and Restricted Covered Data Transactions.** The EO directs the DOJ to identify classes of data transactions that are either prohibited outright, or restricted subject to predefined security requirements to mitigate data access by covered persons and countries of concern. Prohibited transactions would include data-brokerage transactions and transactions involving bulk human genomic data. The contemplated categories of restricted transactions include vendor agreements (e.g., agreements for technology services and cloud-service agreements), employment agreements and investment agreements. However, the DOJ is considering categorically excluding investment agreements that are passive in nature and do not convey ownership interest or rights, including investments by passive limited partners.
- **Security Requirements for Restricted Transactions.** Security requirements for restricted transactions are still under development, but may entail: (i) implementing basic organizational cybersecurity posture requirements; (ii) minimizing, masking or encrypting data, and implementing logical and physical access controls; and (iii) satisfying compliance-related conditions, such as retaining an independent auditor and performing annual testing and auditing of (i) and (ii). Cybersecurity requirements will be established by the Department of Homeland Security's Cybersecurity and Infrastructure Agency, in reliance on certain industry standards including the well-known National Institute of Standards and Technology framework.
- **Limitations, Exceptions and Licenses.** In line with the EO's stated policy goal of minimizing commercial disruption, the EO carves out data exchanged as part of certain business transactions including banking and financial services, capital markets, financial insurance services, and customer due diligence information requirements for compliance with U.S. law. The Proposed Rules also contemplate

exempting transactions that are subject to CFIUS data mitigation arrangements and certain transactions that are subject to U.S. government contracting safeguards — both in an attempt to avoid duplicative regulatory outcomes. Importantly, the EO allows the DOJ to establish an economic sanctions-like licensing regime to provide for general and specific licenses for data transactions that are otherwise prohibited or restricted, and the DOJ contemplates using general licenses to allow for wind-down periods for certain activities.

Six Key Takeaways

The restrictions discussed in the EO and Proposed Rules are not immediately effective, and the eventual final rules will not be retroactive. The contours of the Proposed Rules will likely be amended prior to full implementation based on Congressional and public input. Notwithstanding anticipated change, there *are* some things that potentially impacted companies may consider doing now:

1. **Take Stock of Data.** Kirkland's extensive participation in filings before CFIUS has taught us that many companies underestimate the amount and sensitivity of U.S. person information that they collect and maintain. Particularly given the uncertainty around how the DOJ will ultimately define the threshold for "bulk" data, companies may want to spend time now to take stock of what types of information they collect and maintain, regardless of whether they use that information, and regardless of the fact that they may have extensive role-based restrictions and other protections in place to prevent the vast majority of company personnel from accessing it. Businesses of any size could potentially collect a great deal of data and, in CFIUS reviews, we have found that the DOJ has an appetite for placing rigorous conditions even on small businesses when CFIUS identifies an exploitable risk relating to sensitive data.
2. **Traditionally Non-Identifiable Data is Implicated.** In its Proposed Rules, the DOJ states that it is defining personal data in a way that is "significantly narrower than the broad categories of material typically implicated by privacy-focused regulatory regimes." Nevertheless, companies may want to reevaluate the data they collect from the perspective of this EO and Proposed Rules. Some companies, including companies in the healthcare/life sciences, gaming and other software-driven industries, have access to large amounts of data for which they themselves may not have the means to identify a specific individual. The EO and Proposed Rules currently reference sensitive data that is "reasonably linked to an individual," and data that is "linked and linkable" to government-related persons. However, the EO specifically notes that even data that is seemingly non-

identifiable (e.g., anonymized, pseudonymized or de-identified) is increasingly at risk of being identifiable through the use of advanced technology (including big-data analytics, artificial intelligence and high-performance computing). The DOJ has requested comments regarding whether and how transfers of such data should be restricted (which is particularly notable considering anonymized or de-identified data is exempt from the purview of many privacy regimes). Kirkland will be following the development in both this rulemaking process and in how the DOJ views and reacts to bulk, non (traditionally) identifiable data in other settings.[7]

3. **The Contours of Covered Persons in Complex, Global Business Structures.** Companies that possess U.S. persons' bulk sensitive personal data may want to conduct further diligence to determine whether and how they and their subsidiaries will become subject to this rulemaking, and further determine whether any of their affiliates or personnel will be deemed covered persons. Although the Proposed Rules contemplate exempting "intra-entity transactions incident to business operations,"[8] companies may need to evaluate, and perhaps even modify, their intra-company data sharing agreements. Additionally, an employment agreement with a covered person would be considered a covered data transaction under the Proposed Rules, and thus companies may want to evaluate whether the role of any potentially impacted company personnel would involve access to sensitive personal data. Note that citizens of countries of concern located in the U.S. or in a third country and not primarily resident in a country of concern would not be treated as covered persons under the contemplated definition. However, companies may need to consider employees of parents, affiliates, or even joint ventures and non-wholly owned subsidiaries more closely. The EO warns of risks relating to the cyber, national security and intelligence laws that can obligate private entities and individuals in certain countries to provide data to a country's government. The DOJ may adjust these definitions to further address such risks.
4. **Investment Agreements and the Overlap Between Covered Data Transactions and CFIUS-Covered Transactions.** The DOJ has stated that it does not anticipate that this EO will have significant overlap with existing authorities, with the *significant* exception of investment agreements that qualify both as a covered data transaction under the Proposed Rules and that are also a "covered transaction" subject to CFIUS review. The DOJ may determine not to independently regulate an otherwise prohibited or restricted transaction if CFIUS enters into or imposes an interim order or other mitigation measures to resolve the risk to U.S. national security arising from it (a "CFIUS Action"). Given that the DOJ would generally be leading the effort to formulate the CFIUS Action from their position as a co-lead agency, they would have an opportunity to impose

substantially similar mitigation requirements through the CFIUS process, and the DOJ explains its intent to reduce duplicating regulatory outcomes. However, the DOJ anticipates that it could exercise its authority, under the EO, to restrict transactions that may be under CFIUS review but not yet the subject of a CFIUS Action. This could have impacts on the structure and timing of investments in, from and with covered persons. Although not addressed in the Proposed Rules, Kirkland will be monitoring any developments regarding how a U.S. business that is or becomes subject to a CFIUS national security agreement (e.g., a National Security Agreement, Proxy Agreement or a similar instrument) will be treated with respect to its own subsequent transactions that would otherwise be considered covered data transactions, including whether operating under a CFIUS mitigation agreement would render an otherwise covered person exempt from treatment as such under this EO.

5. **DOJ Recommends a Compliance Framework.** Companies will be required to comply with the final rule as soon as it becomes effective, which means that some companies may want to begin developing a compliance framework in advance of final rules. The Proposed Rules contemplate civil monetary penalties for impacted companies that fail to comply, and a failure to implement a compliance framework could be an aggravating factor in an enforcement action. The DOJ states, in its comments to the Proposed Rules, that it is not going to impose any specific due diligence requirement nor require affirmative reporting or recordkeeping, but does expect companies to "develop and implement risk-based compliance programs." In line with enforcement guidelines under other regulatory regimes, the DOJ intends to consider the effectiveness and quality of these compliance programs in assessing potential penalties. In particular, companies may want to consider their existing data privacy and cybersecurity hygiene and compliance framework in comparison to industry standards generally, and standards noted in the Proposed Rules specifically.
6. **Updated Vendor Diligence.** Clients that collect or maintain sensitive personal data of U.S. persons and use third-party vendors to provide cloud computing, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or Software-as-a-Service (SaaS) products or services may want to conduct proactive vendor diligence to identify whether any of their agreements allow the vendors access to their data, whether the vendors might be deemed covered persons, and if the sensitive personal data could be stored in or accessed from a country of concern. Software companies that contract out all or part of their software development to a covered person should evaluate whether the software development services provided by the covered person involve access to sensitive personal data. Although the Proposed Rules do not impose any data localization requirements, companies that allow vendors to access and store their data from outside of the

> U.S. — including vendors headquartered in European countries, for example — may, in the future, need to ensure that they contractually require those vendors not to re-export that data to a country of concern or covered person.

---

1. Executive Order 13873 on "Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern". https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/ ↩

2. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/ ↩

3. Executive Order 13873 on "Securing the Information and Communications Technology and Services Supply Chain". https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/. The Department of Commerce published an interim final rule under this Executive Order: https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain. ↩

4. For further context on Trump administration actions, see: https://www.kirkland.com/publications/article/2021/07/what-cos-can-do-sensitive-data-regs. ↩

5. Established by EO 13913, https://www.federalregister.gov/documents/2020/04/08/2020-07530/establishing-the-committee-for-the-assessment-of-foreign-participation-in-the-united-states. Related predecessor rulemaking includes Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and the additional measures in Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data from Foreign Adversaries). ↩

6. https://www.justice.gov/opa/pr/justice-department-implement-groundbreaking-executive-order-addressing-national-security ↩

7. From the EO: "Even if such data is anonymized, pseudonymized, or de-identified, advances in technology, combined with access by countries of concern to large data sets, increasingly enable countries of concern that access this data to re-identify or de-anonymize data, which may reveal the exploitable health information of United States persons." ↩

8. The Proposed Rules describe "intra-entity" transactions and then give examples describing transactions between U.S. persons and their affiliates. ↩

Authors

Ivan A. Schlager, P.C.

Partner / Washington, D.C.

John Lynn, P.C.

Partner / Bay Area – San Francisco / Austin

Robert Kantrowitz

Partner / New York

Related Services

Practices

- International Trade & National Security

Suggested Reading

- 15 January 2025 Article Nippon, U.S. Steel Face Long Odds On Merger Challenge
- 02 December 2024 Award Four Kirkland Partners Recognized Among Washingtonian's Top Lawyers 2024
- 21 November 2024 Press Release Kirkland Advises Hg on Significant Investment in Empyrean Solutions