November 4, 2024

# Department of Justice issues proposed rule on US sensitive data sharing with countries of concern

On October 29, the Department of Justice ("DOJ") published in the *Federal Register* a notice of proposed rulemaking that would prohibit or restrict transactions involving bulk sensitive personal data – including personal health data, human genomic data, and biometric identifiers -- between US companies and individuals or entities located in DOJ-designated countries of concern.

The rule implements Executive Order 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, and aims to address national security concerns surrounding countries of concern accessing the sensitive personal data of U.S. consumers and US government-related data. In the proposed rule, DOJ notes there is a risk that countries of concern can use the bulk sensitive data to engage in blackmail or other illicit activities.

While the rule does include a long list of exempted transactions, it holds important implications for industries, including pharmaceutical and medical device companies, that share or transfer large amounts of sensitive data with companies located in countries of concern.

- More information: Press release, Fact sheet, Proposed Rule

Summary of Key Provisions

The proposed rule aims to clarify the types and volumes of bulk sensitive personal data and US government-related data, as well as the types of international transactions that would be prohibited or restricted with entities in "countries of concern" or "covered persons."

The rule designates six countries as countries of concern: China, including Hong Kong and Macau; Cuba; Iran; North Korea; Russia; and Venezuela. DOJ, in the rule, says these countries have "engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of U.S. persons, and pose a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or the security and safety of U.S. persons." DOJ also says these countries present a significant risk of exploiting bulk sensitive personal data or government-related data.

The rule outlines four classes of "covered persons":

- A foreign entity that is at least 50% 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;
- A foreign person that is at least 50% owned, directly or indirectly, by a covered person
- A foreign individual who is an employee or contractor of a country of concern or entity deemed to be a covered person;

- A foreign individual who primarily resides in the territorial jurisdiction of a country of concern.

DOJ in the rule identifies two categories of prohibited covered data transactions and three categories of restricted covered data transactions. Prohibited covered data transactions are data brokerage transactions and transactions involving access to bulk human genomic data or biospecimens from which genomic data can be derived. Restricted covered data transactions are vendor, employment, and non-passive investment agreements. These types of transactions must comply with security requirements developed by the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA). The rule also seeks to prevent data from being resold or transferred to countries of concern through third-parties by requiring US persons or entities engaged in data brokerage with any foreign person who is not considered a covered person to follow certain processes, such as including language in the contract prohibiting the data from being resold or shared with a country of concern or a covered person.

DOJ in the rule also outlines the types and volumes of sensitive person data transactions that would be subject to prohibitions or restrictions. DOJ said the prohibitions or restrictions would apply to any amount of sensitive personal data – including anonymized, pseudonymized, de-identified, or encrypted data – that exceeds the below thresholds in aggregate over the preceding 12 months before a "covered data transaction":

- Human genomic data of more than 100 U.S. persons;
- Biometric identifiers of more than 1,000 U.S. persons;
- Precise geolocation of more than 1,000 U.S. devices;
- Personal health data of more than 10,000 U.S. persons;
- Personal financial data of more than 10,000 U.S. persons;
- Covered personal identifiers of more than 100,000 U.S. persons; or
- Combined data where any individual data type meets the threshold number of persons or devices collected or maintained in the aggregate for the lowest number of U.S. persons or U.S. devices in that category of data.

The rule also includes a list of exempted transactions, including drug, biological product, and medical device transactions involving "regulatory approval data" required to obtain or maintain regulatory approval in a country of concern and certain clinical investigations and post-market surveillance data. The rule also authorizes DOJ to issue general licenses to authorize certain prohibited or restricted transactions under specific conditions.

US persons and entities would be expected to develop and implement compliance programs based on their individualized risk profiles. U.S. persons or entities that engage in a restricted transaction would need to comply with new compliance obligations, including implementing risk-based procedures to verify and log data flows and sensitive personal and government-related data types and volume, and vendor identities. The rule also includes new reporting requirements for those engaged in restricted transactions and those who received and rejected a prohibited transaction. DOJ said violations of the rule could result in civil monetary penalties and willful violations can result in criminal fines.

*If you have questions, please contact Heather Meade or Heather Bell.*

**Washington Council Ernst & Young**

Washington Council Ernst & Young (WCEY) is a group within Ernst & Young LLP that combines the power of a leading professional services organization with on-the-ground knowledge, personal relationships and attention to detail of a boutique policy firm. We provide our clients with timely, relevant Washington insight and legislative advisory services customized to their needs. To learn more, contact wcey@ey.com.