CLIENT ALERTS & INSIGHTS

DOJ Proposes Rules Limiting Transfer of Sensitive Data to Countries and Individuals

DECEMBER 12, 2024

Authors: Michael D. Stovsky, Kristopher J. Chandler

Pursuant to President Biden's March Executive Order, the DOJ has proposed new rules limiting the transfer of certain categories of data to "countries of concern" or "covered persons".

In late October, the Department of Justice issued a new proposed rule that would implement regulations prohibiting the transfer of certain categories of bulk data about U.S. individuals to persons entities, or locations connected to "counties of concern", which include China, Cuba, Iran, North Korea, Russia, and Venezuela. The rule is made pursuant to Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern". The executive order called on the US Department of Justice and relevant federal agencies to build out requirements surrounding the transfer of specific categories of personal data to "countries of concern" and "covered persons" as defined in the rule.

While the U.S. still lags behind other prominent jurisdictions-such as the European Union, United Kingdom, and China-in that the U.S. lacks a comprehensive federal level cross-border data transfer regulation, the U.S. has stepped up measures related to national security. This proposed rule is the latest update in furthering that trend.

The proposed rule covers broad categories of data and a broad swatch of data transactions and transfers. At a high level, any U.S. business involved in data transactions and transfers will need to take note as the proposed rule regulates and puts requirements in place for any transaction dealing with U.S. government-related data or bulk sensitive personal data. The proposed rule bans the transfer of U.S. government-related data or bulk sensitive data to the countries of concern, which currently include China, Cuba, Iran, North Korea, Russia, and Venezuela in certain types of transactions, and heavily regulates the transfer of sensitive personal data in other types of transactions placing extensive cybersecurity compliance and control requirements on the transferor.

See more below for information on key terms, prohibitions, and requirements under the proposed rule.

Important Definitions

The first key to understanding the proposed rules is to understand the types and categories of data it regulates. The proposed rule focuses on two categories of data: (1) bulk sensitive personal data; and (2) U.S. government-related data.

"Sensitive personal data" is defined under the proposed rule to include human genomic data, biometric identifiers, precise geolocation data, personal health data, personal financial data, and-the broadest sub-category-covered personal identifiers. "Covered personal identifiers

" is subsequently defined to include government identification numbers (e.g., Social Security numbers), financial account numbers or personal ID numbers associated with a financial service, device-based identifiers such as IMEIs, SIMs or MAC addresses, demographic or contact data, advertising identifiers, account credentials, network identifiers (e.g., IP addresses), and CPNI.

Importantly, the proposed rule provides key exceptions to the otherwise broadly defined "covered personal identifier" category. The following is the list of data that would **not** be considered covered and therefore not considered sensitive:

- Demographic or contact data that is linked only to other demographic or contact data (such as first and last name, birthplace, ZIP code, residential street or postal address, phone number, and email address and similar public account identifiers); and
- A network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifier, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar service.

"U.S. government-related data" is defined under the proposed rule as any data that either (1) is considered precise geolocation data for any of the DOJ's designated Government-Related Location data List; or (2) any amount of sensitive personal data that is marketed as linked or linkable to current U.S. government current or former employees, contractors, or officers.

Prohibitions & Restrictions

The proposed rule then goes on to (1) prohibits data transactions or transfers with respect to bulk sensitive personal data and U.S. government-related data where "countries of concern" or "covered persons" are involved; and (2) restricts any data transactions or transfers with respect to bulk sensitive personal data and U.S. government-related data unless certain requirements are met.

First and foremost, the proposed rule generally prohibits the entities from engaging in covered data transactions to "countries of concern" or to "covered persons". "Covered data transactions" is subsequently defined as "any transaction that involves any access to any government-related data or bulk U.S. sensitive personal data."

Where U.S. government-related data is involved in a transaction or data transfer, the prohibitions and restrictions apply without regard to the size of the deal. However, sensitive personal data transactions or transfers must be a certain size-rather contain a certain quantity of data-before the prohibitions and restrictions apply. A transaction involves "bulk" sensitive data if any of the following thresholds are met:

- Human genomic data à more than 100 U.S. individuals
- Biometric identifiers à more than 1,000 U.S. individuals
- Precise geolocation data à more than 1,000 U.S. individuals
- Personal health data à more than 10,000 U.S. individuals
- Personal financial data à more than 10,000 U.S. individuals

- Covered personal identifiers à more than 100,000 U.S. individuals

The full prohibition on transfers to countries of concern or to covered persons covers sanctioned countries-such as Russia, North Korea, Iran, China, and Venezuela-and entities owned by, incorporated or formed in, or located in, such sanctioned countries. The definition of "covered person" under the proposed rule extends to:

- any entity that is 50% or more owned by a country of concern;
- an entity or person that is an employee or contractor of a country of concern;
- an entity or person that is a primary resident in the jurisdiction of a country of concern;
- any entity or person the Attorney General determines to have acted or purported to act on behalf of a country of concern.

The broad, ambiguous nature of the "covered person" definition and prohibition on transacting in bulk data transfers has potential to greatly impact economic activity between U.S. businesses that deal with cross border data transfers between-for example-the U.S. and China. The strict nature of the proposed rule has potential to see U.S. businesses turn to data localization in lieu of cross-border data transfers. Data localization (e.g., storing a countries personal data in data centers and on cloud instances / servers located in that country) is a growing trend in other jurisdictions as countries like China or regions like the EU have increased cross-border data transfer regulations.

Beyond transfers of data to countries of concern-or persons or entities located in or related to countries of concern-the rule goes one step further and restricts any covered data transaction to any non-U.S. person or entity. If a U.S. business engages in a transaction or transfer of U.S. government-related data or bulk sensitive personal data to any non-U.S. person or entity (including, for example, an entity that is located in the U.S., but owned by a country of concern or a covered person located in a country of concern), it must first meet the following requirements:

1. contractually require the receiving entity to refrain from engaging in a subsequent covered data transaction of the same data to a country of concern or covered person; and
2. report any known or suspected violations of this requirement.

Importantly, there are some exceptions that could ease the restrictive nature of the proposed rule. The following are not restricted or prohibited under the proposed rule:

- **Personal Communications**: personal communications not involving the transfer of anything of value.
- **Informational Material**: information and informational materials imported or exported to or from any country.
- **Travel**: data transfers that are ordinary and incidental to travel to or from any country

- **S. Government**: data transfers or transactions that are conducted as the official business of the U.S. government.
- **Financial Services**: data transfers or transactions to the extent they are ordinary and incidental to the provision of financial services.
- **Corporate Group Transfers**: data transfers or transactions to the extent they are ordinary and incidental to administrative or ancillary business operations (e.g., HR, payroll, customer support, employee benefits).
- **Federal Law**: data transfers or transactions required or authorized by federal law.
- **CFIUS**: data transfers or transactions to the extent they involve an investment agreement subject to CFIUS (the Committee on Foreign Investment in the United States) action.
- **Telecommunications**: data transfers or transactions-other than those involving data brokerages-to the extent they are ordinary and incidental to and part of the provision of telecommunication services.
- **Medical Uses**: de-identified sensitive personal data required to obtain or maintain authorization or approval of medical research or medical products (including pharmaceutical).
- **FDA**: data transfers or transactions ordinary and incidental to FDA clinical investigations.

Security Requirements

The proposed rule also would act to impose broad security requirements on any U.S. business conducting regulated transactions or transfers-with the base requirement being that any such business is required to develop and implement a comprehensive data compliance/security program that covers the following:

1. Risk-based procedures for verifying data flows involved in any restricted transaction, including procedures to verify and log, in an auditable manner, the following:

    a. The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;

    b. The identity of the transaction parties, including any ownership of entities or citizenship or primary residence of individuals; and

    c.The end-use of the data and the method of data transfer;

2. For restricted transactions that involve vendors, risk-based procedures for verifying the identity of vendors;

3. A written policy that describes the data compliance program and that is annually certified by an officer, executive, or other employee responsible for compliance;

4. A written policy that describes the implementation of the security requirements and that is annually certified by an officer, executive, or other employee responsible for compliance; and

5. Any other information that the Attorney General may require.

The annual audits must be conducted by a qualified, independent third party and **cannot** be an internal auditor.

The proposed rule also incorporates some baseline standard security requirements under federal cybersecurity standards and frameworks such as NIST and ISO frameworks.

Additionally, the proposed rule would implement a broad recordkeeping requirement. The proposed rule requires a U.S. business to maintain a full and accurate record of each covered / regulated transaction or data transfer engaged in for a period of 10 years after the date of the regulated transaction or data transfer. Under the proposed rule, the following must be kept in an auditable manner:

1. A written policy that describes the data compliance program and that is certified annually by an officer, executive, or other employee responsible for compliance;
2. A written policy that describes the implementation of any applicable security requirements and that is certified annually by an officer, executive, or other employee responsible for compliance;
3. The results of any annual audits that verify the U.S. person's compliance with the security requirements and any conditions on a license;
4. Documentation of the due diligence conducted to verify the data flow involved in any restricted transaction, including:

    a. The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;

    b. The identity of the transaction parties, including any direct and indirect ownership of entities or citizenship or primary residence of individuals; and

    c. A description of the end-use of the data;

5. Documentation of the method of data transfer;

6. Documentation of the dates the transaction began and ended;

7. Copies of any agreements associated with the transaction;

8. Copies of any relevant licenses or advisory opinions;

9. The document reference number for any original document issued by the Attorney General, such as a license or advisory opinion;

10. A copy of any relevant documentation received or created in connection with the transaction; and

11. An annual certification by an officer, executive, or other employee responsible for compliance of the completeness and accuracy of the records documenting due diligence.

The proposed rule also has some automatic reporting requirements. Covered U.S. businesses that engage in restricted transaction involving cloud-computing services and that has 25% or more of the entity equity interests owned by a country of concern or covered person must make annual reports to the U.S. government.

Penalties

With respect to any violation of the proposed rule, a civil penalty would apply and would be set the greater of: (i) $368,136 per violation; or (ii) an amount twice the size of the transaction that is the basis of the violation. Willful violations of the proposed rule can additionally result in criminal penalties of fines up to $1,000,000 or up to 20 years in prison.

Conclusion

With the U.S. lacking a broad, federal level data privacy law or cross-border data transfer regulation, this proposed rule and Executive Order 14117 are the U.S.'s first substantial foray into cross-border data transfer regulation.

This new proposed rule and the Executive Order mark a clear understanding by the federal government that regulating personal data and transfers thereof are critical. They impose substantial new due diligence obligations on U.S. businesses, and U.S. U.S. companies that transmit, store, or process utilizing the services of third party vendors will need to maintain keen eyes on the rulemaking process as new final regulations may impose significant new obligations and penalties.

The Department of Justice is aiming for the rule to be finalized in early 2025.

As the U.S. federal government and U.S. state governments continue to implement new-and amend existing-data protection requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Michael Stovsky at mstovsky@beneschlaw.com or 216.363.4626

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.

Kris Chandler at kchandler@beneschlaw.com or 614.223.9377.