3 Jan. 2025

OPINION

International Data Transfers | Law & Regulation

A view from DC: Ready for new US restrictions on nearly all foreign access to personal data?

Cobun Zweifel-Keegan
IAPP staff
CIPP/US, CIPM
8 Minute Read

As the new year turns, the Biden administration is rushing to complete its top priorities before the Trump administration takes over 20 Jan. Possibly the most watched end-of-year development related to personal data has been the U.S. Department of Justice's rulemaking on "preventing access to U.S. sensitive personal data and government-related data by countries of concern or covered persons."

After publishing an updated draft rule in October 2024, it was widely expected the DOJ would publish the final rule before the end of the administration. And behold, the agency delivered a final rule just after Christmas.

This is the culmination of a series of events set in motion by Executive Order 14117, which distills the Biden administration's attempt to respond to national security concerns around the risk of access to sensitive personal data by "countries of concern."

Though the regulation primarily focuses on direct transactions to persons associated with six countries, China, Cuba, Iran, North Korea, Russia and Venezuela, it also has implications for all foreign transactions. There is a lot for privacy pros to unpack, as the rule includes possibly the broadest definition of "sensitive data" of any legal code and a complex set of interlocking inclusions and exclusions.

The DOJ's accompanying fact sheet does a good job of explaining how the final rule differs from the Notice of Proposed Rulemaking, which I previously wrote about under the headline "the beginning of the end of the free flow of data."

U.S. entities should be prepared to conduct an in-depth multi-part analysis on every transaction to fully comport with the rule.

Does the transaction include a foreign entity?

The substantive obligations in the final data security rule mean that U.S. companies — and U.S. subsidiaries of foreign entities — must first be able to identify any transaction that could allow access to covered data by a foreign entity. The rule refers to "data brokerage transactions," but this is broadly defined to include any type of transaction that provides access to personal data by an entity that "did not collect or process the data directly from the individuals linked or linkable to the collected or processed data."

I am intentionally using the phrase "foreign entity" here to highlight the breadth of the obligations. For transactions involving entities who are not affiliated with countries of concern — and are not otherwise identified on a list by the DOJ — U.S. companies must include contractual terms that restrict the onward transfer of covered data to such entities whenever the DOJ rules are triggered.

On top of this, the rule creates an obligation for U.S. companies to submit what one might call a snitch report to the DOJ when they know or suspect their foreign partner has violated these contractual terms.

Can the foreign entity access US personal data because of this transaction?

As a transaction-based regime, the new DOJ program does not adopt the type of logic one would expect for restrictions on the cross-border transfer of personal data. In fact, in a formulation that probably more accurately reflects technical reality than the usual border-based restriction, "transfer" of data is not required to trigger the rules. All that is required is a transaction enabling access to data.

In fact, the DOJ includes an illustrative example of an AI chatbot that could be used to reproduce covered data when responding to prompts. If the U.S. company that licenses the chatbot, even to its own foreign affiliate, knows or should know the service could be used to provide access to covered data, the transaction must meet requirements under these rules.

Is the accessible US personal data protected under the data security rule?

Of course, the scope of the rule is limited by the type of data involved. But the definitions of sensitive data in the rule do not comport with anything we have ever seen in the privacy world.

This bears repeating as many times as I possibly can. This rule is not about traditional categories of sensitive information and the DOJ explicitly rejects narrower formulations proposed by commenters.

To my mind, the best way to document compliance with the rule is to ensure that each covered type of data is excluded from the product, service or transaction in question. In many situations, this will be impossible.

Start with the easy exclusions. Government-related data should always be excluded. There are no threshold requirements for this type of information; even a single data point can trigger the prohibitions. There are two types: location data about government facilities and "any sensitive personal data, regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the U.S. government."

So, two operational requirements are embedded here. Location datasets must be scrubbed of all government facilities, using exclusion lists to be provided by the U.S. government. And no company may market sensitive personal data as linkable to government individuals.

Does the protected data type meet the relevant bulk threshold or any exclusions?

This brings us to the categories of sensitive personal data. Again, they appear more straightforward than they are: "covered personal identifiers, precise geolocation data, biometric identifiers, human genomic data, personal health data, personal financial data, or any combination thereof."

When not associated with government individuals, each of these categories of sensitive data comes with its own threshold to meet the "bulk" volume restrictions under the rule, ranging from 100 to 100,000 U.S. persons, depending on the perceived riskiness of the data type. Each of these is worthy of its own analysis, especially financial and health data, which are unlikely to neatly fall into existing compliance requirements for U.S. sectoral privacy laws.

For now, I will focus again on the broadest category here,"covered personal identifiers," which is only triggered by the highest threshold. The rule to remember here: it takes two.

Any single "listed identifier" if accessed with another listed identifier — or even if accessed with another piece of information that "is disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data" — counts as sensitive personal data.

Listed identifiers include eight categories ranging from government ID numbers to device information like MAC addresses and advertising IDs to network information like IP addresses to contact information like address, email, phone or ZIP code.

Any transaction that enables two of these identifiers to be linked falls within the restrictions of the data security rule if it does so for 100,000 or more U.S. persons.

As one example, many third-party cookies and other web trackers collect some form of device ID together with some form of network ID. The DOJ rules treat these two identifiers together as sensitive data.

To my mind, nearly every ongoing digital commercial activity may need to be reviewed for compliance, even if that means verifying an exempt status. As with all U.S. privacy regulations, public data is excluded from the requirements. So are communications data and expressive materials with associated metadata.

Do you know your customer?

If thresholds do not fully exempt a U.S. entity's transactions from the rule, it must be exceedingly careful to document the customers on the other end of the transaction. As already mentioned, any foreign person receiving access to a sufficient volume of covered data must be subject to a contract with onward transfer restrictions.

Further, the definition of "covered persons," that is, entities associated with countries of concern, is quite broad, including any resident of those countries and any entity with 50% or more ownership by a covered person. Receiving adequate documentation of ownership — or at the very least contractual safeguards that these rules do not apply — will need to be a standard part of all U.S. data transactions moving forward.

The DOJ has promised to publish "compliance, enforcement, and other guidance" on a dedicated webpage. This is likely to include standard contractual language, though the timing for publishing any guidance is uncertain.

Even if not a prohibited transaction, is the data access nonetheless restricted?

The DOJ rules implement the vision of Executive Order 14117 to include mandatory data security safeguards for additional categories of transactions, including vendor agreements, employment agreements and investment agreements.

These are known as "restricted transactions," and in order to be authorized they must soon comply with the security requirements recently published in draft form by the U.S. Cybersecurity and Infrastructure Security Agency. CISA is expected to finalize these requirements soon.

A notable feature of this structure is the intentional inclusion of anonymized, pseudonymized or deidentified data within the definition of sensitive data in the final rule. Deidentification is not a get-out-of-jail-free card.

Instead, as the DOJ puts it, by requiring companies engaging in restricted transactions to meet the specifications laid out in CISA's security requirements "to the extent such methods are sufficient to fully and effectively prevent access to covered data that is linked or identifiable (or unencrypted or decryptable), the rule promotes effective methods while prohibiting ineffective methods."

The DOJ claims the new requirements will not cause a major burden for multinationals and other companies with robust compliance programs. It is certainly true that data mapping and mature privacy compliance operations will set companies up for success under this rule, but at the same time this is like no U.S. obligation we have ever seen in the privacy sphere.

In short, the final data security rule signals the beginning of a new era of U.S. data flow compliance obligations, with contractual, technical and legal requirements for most digital activities. The rule will go into effect 90 days after it is published in the federal register, likely sometime in March 2025.

Please send feedback, updates and restricted transaction flowcharts to cobun@iapp.org.

Cobun Zweifel-Keegan, CIPP/US, CIPM, is the managing director, Washington, D.C., for the IAPP.

This article is eligible for Continuing Professional Education credits. Please self-submit according to CPE policy guidelines.

Submit for CPEs

Interested in writing for us? Visit our Contributor Guidelines Page →

Related stories

- A view from DC: Watergate and the Privacy Act of 1974
- A view from DC: Geolocation enforcement trends include broad lessons for US privacy teams
- A view from DC: CFPB calls for states to regulate financial privacy
- Biometrics in the EU: Navigating the GDPR, AI Act
- Data governance: Why this year is different from all others

About

The IAPP is a policy neutral, not-for-profit association founded in 2000 with a mission to define, promote and improve the professions of privacy, AI governance and digital responsibility globally.




Contact us

Press

Advertise

Become a member

The IAPP is the only place you'll find a comprehensive body of resources, knowledge and experts to help you navigate the complex landscape of today's data-driven world. We offer individual, corporate and group memberships, and all members have access to an extensive array of benefits.

Pease International Tradeport, 75 Rochester Ave., Portsmouth, NH 03801 USA • +1 603.427.9200