Articles + Publications | February 18, 2025

Do You Know Where Your Data Is Going? On April 8, New National Security Rules Take Effect

WRITTEN BY

Peter E. Jeydel | James Koenig | Laura Hamady | Ryan Last | Joel M. Lutz

A groundbreaking new regulatory regime, imposing rules unlike any in existing U.S. law, may surprise many companies due to its sudden adoption and complexity. This article tries to simplify the changing regulatory landscape, highlighting key points for any company with a U.S. presence that may be transferring data abroad.

On January 8, the U.S. Department of Justice's (DOJ) National Security Division (NSD) released its final rule, regulating access to sensitive U.S. data by "countries of concern," *i.e.*, China (including Hong Kong and Macau), along with Russia, Iran, North Korea, Cuba, and Venezuela, or by "covered persons" anywhere in the world that are linked to those countries. This final rule comes in response to rising concerns over these governments' exploiting sensitive U.S. personal data and government data for purposes such as espionage. The final rule closely aligns with the DOJ's earlier proposed rule.

The final rule sets out a sweeping data security regime based on national security policy. It is important to understand that this is not like traditional data privacy regimes; for example, there is no exception to the restrictions based on consent. In many cases, contractual provisions alone will not suffice as a compliance approach. Rather, these are in some respects much more stringent rules that stem from U.S. national security concerns. Therefore, companies should not be comfortable that their activity is compliant with the final rule merely because it satisfies other existing data privacy and security laws. These new regulations are a different ballgame altogether and will often require very challenging steps to be taken, such as changes to existing data security practices and business processes. When applicable, these steps need to be in place by April 8 — a very short timeline.

There are some big carve-outs that will provide relief for many companies. For example, these new regulations do not apply to activity that takes place entirely within the United States among U.S. persons, even if they are owned or controlled by Chinese or other non-U.S. persons (unless they are specifically designated by DOJ). But the rules can cover, for example, U.S. companies that share data with their own affiliates (or third parties) in China or elsewhere, as well as commercial data licensing and other forms of data access across borders. Even for companies that may ultimately fall under one or more carve-outs, it is important to assess and document those positions, and be prepared to answer questions from DOJ.

The core of the final rule is set to take effect on April 8. There is no indication at this point that the Trump administration intends to change course, and, in light of the China and national security focus of the final rule, we expect it to move forward. Given the complexity of the final rule, this is a very short timeline for companies that are not already deep into their preparations for compliance with these regulations. DOJ has provided a delayed

implementation timeline, until October 5, for certain requirements under the final rule (*i.e.*, affirmative due diligence, auditing and reporting obligations). Additionally, DOJ has indicated they could potentially provide a degree of flexibility in extenuating circumstances (*e.g.*, by the issuance of authorizations or guidance). Nonetheless, companies that may be impacted by these rules should move urgently to bring themselves into compliance or analyze and document the non-applicability of these rules, in order to be in a strong position with the regulator prior to April 8.

The final rule is similar to — but distinct in important ways from — the 2024 Protecting Americans' Data from Foreign Adversaries Act (PADFA), administered by the Federal Trade Commission (FTC). PADFA is focused on "data brokers," whereas the DOJ final rule applies to a much broader array of companies and transactions, including vendor agreements, employment agreements, and investment agreements that do not involve data brokering. Moreover, PADFA includes broad carve-outs that are not present in the final rule, such as for the provision of services where the data transfers are only ancillary to the services provided. On the other hand, the DOJ final rule has a more limited scope when it comes to covered data, which must meet specified "bulk" thresholds. There are other differences between the laws, but both carry consequential compliance obligations. Companies should carefully review (or refresh) their data maps and analyze their data types and flows in light of PADFA and the DOJ final rule to ensure they understand if either or both of these new sets of requirements could impact their compliance approach.

Scope of the Final Rule

The final rule generally applies to U.S. persons that "knowingly" provide "access" (very broadly defined) to listed types of covered data involving a country of concern or covered person.

These restrictions can apply to activity involving the U.S. and a third country (*e.g.*, Singapore, the UK, or any other country that is not a "country of concern"), when there are certain links to a country of concern (*e.g.*, a "covered person" that is owned by a Chinese entity). But these rules generally do not apply to activity that is 100% located in the U.S., even when conducted by persons linked to a country of concern.

The key elements that must be met for the main restrictions under these rules to apply are as follows:

- **Covered Data**: This includes the types of data listed below where the specified volume thresholds are met (except for U.S. government-related data, any amount of which triggers the rules) at any point in the preceding 12 months, whether through a single transaction or aggregated across several transactions involving the same parties:
    - Human genomic data: more than 100 U.S. persons;
    - Other human `omic data: more than 1,000 U.S. persons;
    - Biometric identifiers: more than 1,000 U.S. persons;
    - Precise geolocation data: more than 1,000 U.S. devices;

- Personal health data: more than 10,000 U.S. persons;
- Personal financial data: more than 10,000 U.S. persons; or
- Covered personal identifiers: more than 100,000 U.S. persons.

For combinations of these types of data, the lowest applicable threshold applies.

Even if data is anonymized, pseudonymized, de-identified, or encrypted, it is still covered (though such measures will be relevant in implementing the Security Requirements, as discussed below).

There can be complexities (including important carve-outs) built into these definitions of covered data. For example, "personal identifiers" are not covered if they are not linked or linkable in specified ways to other covered data. Dissecting these nuances can be hugely important for determining that certain types of data flows are not subject to these rules at all.

- **Knowingly**: The final rule only applies in the first instance to covered activity that is conducted "knowingly," which includes situations where a person "reasonably should have known" of the relevant facts. This means, for example, that electronic services or platforms would generally not be responsible for the activities of their customers (*e.g.*, an email provider whose user emails covered data to a covered person). But DOJ will expect risk-based due diligence and controls around this.

- **U.S. Person**: This includes U.S.-based entities, U.S. citizens or "green card" holders, and any person with asylum or refugee status granted by the U.S. government. (These categories are consistent with U.S. export control rules.) But also (unlike under U.S. export controls), a U.S. person includes "any person in the United States." For example, Chinese or Russian citizens located in the U.S. would be treated as U.S. persons and would not be covered persons (unless individually designated by DOJ). Those individuals may require U.S. export control licensing if they have access to controlled technology (*i.e.*, "deemed exports"), but they would not trigger the applicability of this DOJ final rule. This is an important limitation to the final rule that will facilitate compliance in some cases.

- **Covered Persons**: This includes an individual or entity that is not a U.S. person and that is:
  - An individual primarily resident in a country of concern;
  - An employee or contractor of a country of concern or a covered person entity;
  - An entity based in a country of concern; or
  - An entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by countries of concern or covered persons. (This aligns with the U.S. sanctions (OFAC) "50% rule.")

In addition, DOJ can designate any person as a covered person (*e.g.*, if a person is determined to be acting on behalf of China or another country of concern, or to be violating these rules). So DOJ may in the future develop such a "blacklist." That list may then need to be incorporated into restricted party screening procedures (*e.g.*, if currently in place for OFAC compliance).

The final rule essentially divides transactions into the following five categories: not covered, prohibited, restricted, exempt, and licensed.

- **Non-Covered Transactions**: If any of the key elements of the rules are not met (*e.g.*, there's no U.S. person, no covered person, no covered data, no "access" to covered data, etc.), the final rule is not applicable at all. This goes without saying, but as a practical point it is critical to confirm in the first instance whether each of the elements of a prohibition or restriction is met, as there are significant carve-outs built into these basic elements. For transactions that are not covered, even the final rule's recordkeeping requirements do not apply. However, if there is any nuance involved in determining that the final rule is inapplicable, a record of that analysis should be kept for at least 10 years as a best practice and protective measure in case DOJ comes knocking.

- **Prohibited Transactions**: The final rule prohibits covered transactions involving "data brokerage," which may extend well beyond what many companies would normally think of as data brokerage. DOJ has defined this term as:

the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or a vendor agreement, involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.

This is quite a broad and vague definition that will leave many situations that are not vendor, employment, or investment agreements in a grey area — DOJ has stated that the transaction must be "commercial" in nature (*i.e.*, must involve some form of compensation or consideration), but that still leaves many types of normal commercial partnerships potentially covered.

Critically, the prohibitions on data brokerage include transactions with non-covered foreign persons in third countries (*i.e.*, where there is no specific link at all to China or another country of concern or covered person), unless the U.S. person: (1) contractually requires the foreign person to refrain from engaging in a subsequent covered data brokerage transaction involving the same data with a country of concern or covered person; and (2) reports any known or suspected violations of this contractual requirement within 14 days. This is among the few instances under these regulations when contractual provisions are the focus of the compliance expectation, as compared to implementing security measures or business process changes to satisfy the Security Requirements, which are discussed below. But even here mere contractual provisions are not sufficient, and DOJ expects adherence to those commitments to be monitored and suspected violations to be reported.

In addition to data brokerage, the final rule prohibits the following:

Covered transactions involving “human `omic data” or human biospecimens from which such data could be derived. Companies with such data are on a very tight leash with DOJ and must take a careful compliance approach under these rules.

Evasion, causing violations, and conspiracy (and “knowingly directing” violations): The DOJ personnel who will be enforcing these regulations are part of the same organization — and will share a mindset — with U.S. sanctions and export controls prosecutors. The underlying statutory authority is also the same as that which underlies most U.S. sanctions, which is where most of these particular prohibitions come from. So any efforts to circumvent these rules should be expected to meet with an aggressive enforcement response. A good rule of thumb is to apply these rules based on their letter and spirit, and not to play games or seek “paper compliance” where the reality is the requirements are not being met. Similarly, trying to work around the rules by conducting covered transactions in a non-compliant manner through contractors, business partners, etc., may be high-risk, and concealing activity from partners or other parties can also lead to liability.

- **Restricted Transactions**: Covered transactions that involve vendor agreements, employment agreements, or investment agreements are “restricted,” meaning that they are prohibited unless the U.S. person complies with the stringent “Security Requirements” established by the Cybersecurity and Infrastructure Security Agency (CISA), which is part of the U.S. Department of Homeland Security (DHS). The Security Requirements are discussed in more detail below. Where applicable, the Security Requirements will often prove to be hugely challenging to comply with. In addition, when conducting restricted transactions, there are due diligence, audit, reporting, and recordkeeping requirements that apply and that may be quite burdensome.

    - Excluded investment agreements: While the definitions of vendor agreement and employment agreement are fairly straightforward, there are carve-outs built in to the definition of investment agreement that in essence exclude passive investments, as well as investments in certain non-U.S. assets.

- **Exempt Transactions**: The final rule contains several exemptions, most of which are quite broad. However, in their breadth they leave a lot of gray area, which may create considerable discomfort for many businesses seeking certainty in this high-stakes national security regulatory area. In most (but not all) cases, certain reporting requirements of the final rule still apply to exempt activity. The exemptions cover:

    - Transactions that are “required or authorized by Federal law or pursuant to an international agreement to which the United States is a party,” or by certain global health frameworks, as well as transactions that are “ordinarily incident to and part of ensuring compliance with any Federal laws and regulations.”

    - Another exemption covers transactions that are for official U.S. government business, including government contracting and federally funded research.

    - Corporate group transactions: This exemption is relatively broad, but contains critical limitations. It applies to transactions “[b]etween a U.S. person and its subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction, or control of) a country of concern” that are “[o]rdinarily incident to and part of administrative or ancillary business operations.”

- Financial services: This exemption is also broad but with important limitations. It applies to transactions that are "ordinarily incident to and part of the provision of financial services."

- Telecommunications services: This exemption is similarly broad (though it excludes data brokerage), covering transactions that are "ordinarily incident to and part of the provision of telecommunications services."

- There is another exemption for transactions that involve investment agreements that are "subject to a CFIUS action."

- Drug, biological product, and medical device authorizations: Certain types of data are exempt if the transaction is "necessary to obtain or maintain regulatory authorization or approval to research or market a drug, biological product, device, or a combination product."

- Other clinical investigations and post-marketing surveillance data: Transactions are exempt in certain cases if they are "[o]rdinarily incident to and part of" clinical investigations regulated by the FDA or clinical investigations that support applications to the FDA for research or marketing permits for drugs, biological products, devices, combination products, or infant formula, or are "[o]rdinarily incident to and part of the collection or processing of clinical care data indicating real-world performance or safety of products, or the collection or processing of post-marketing surveillance data (including pharmacovigilance and post-marketing safety monitoring), and necessary to support or maintain authorization by the FDA, provided the data is de-identified or pseudonymized."

- The final rule also reflects the exemptions in the underlying statutory authority (IEEPA) for (1) "personal communications" that do not "involve the transfer of anything of value," (2) the international exchange of "information or informational materials," and (3) transactions that "are ordinarily incident to travel to or from any country." These are the same statutory exemptions as apply under most U.S. sanctions programs. We would expect these exemptions to be construed narrowly and only to be relevant in limited circumstances.

- **Licensed Transactions**: In rare instances, U.S. persons may be able to obtain a license to conduct otherwise prohibited activity (including not fully implementing the Security Requirements or other obligations for a restricted transaction). The DOJ has indicated it may consider issuing general licenses in certain instances, *e.g.*, where market participants may require more time to wind down otherwise prohibited activity. Parties may also submit applications to the DOJ for specific licenses that cover particular intended transactions. The DOJ intends to issue separate instructions on how to apply for a specific license and the criteria that will be applied. We would expect that such license applications will be reviewed quite strictly, and it will be important to make the case that the request is consistent with U.S. national security interests.

Security Requirements

For restricted transactions that are not licensed or exempt, companies must comply with the Security Requirements promulgated by CISA. If the Security Requirements are not properly implemented, such transactions are prohibited. Transactions that are generally prohibited (*e.g.*, involving data brokerage or human

`omic data or related biospecimens) cannot be authorized by complying with the Security Requirements – those are strict prohibitions that can only be overcome with a license (or an applicable exemption). The Security Requirements only come into play for vendor agreements, employment agreements and investment agreements, and where an exemption does not apply.

The Security Requirements in essence require the data to be "fully and effectively" blocked from access by a country of concern or covered person. This is a highly demanding requirement that will be quite challenging to meet in many cases. In addition, the Security Requirements impose a number of organizational-level and system-level requirements that are broadly consistent with the existing obligations and practices of many types of organizations (*e.g.*, regulated financial institutions), but with a few important nuances that are particular to the DOJ final rule.

The most challenging part of the Security Requirements are generally going to be the data-level requirements, which require the U.S. person to "implement a combination of [specifically listed categories of] mitigations that, taken together, is sufficient to fully and effectively prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern." The types of measures that can be employed to achieve this required end result include data minimization, encryption, access controls, and others, with specified requirements (*e.g.*, with respect to management of encryption keys when relying on encryption). At the end of the day, whichever combination of measures is used, this highly demanding standard must be met, and the burden is on the regulated U.S. person to establish that it is met.

For data that does not meet the data-level security requirements, "logical and physical access controls" must be put in place "to prevent covered persons or countries of concern from gaining access" to such data.

The effectiveness of the data-level measures determines whether they are compliant: CISA says that, if "a combination of security mechanisms proves to be insufficient to prevent such access, that combination of security mechanisms will be considered invalid in protecting future access to covered data by covered persons." So testing the effectiveness of the measures, and adjusting them as needed (*e.g.*, based on the company's own risk assessment, technological developments and business process changes) will be important.

Recordkeeping, Reporting, Due Diligence, and Audit Requirements

There is a broad, 10-year recordkeeping requirement under the final rule. This is consistent with the new, 10-year recordkeeping requirement that will soon apply under U.S. economic sanctions regulations, but longer than the five-year recordkeeping requirement that applies under U.S. export controls.

In addition, there are specific requirements regarding due diligence, audits, and reporting (*e.g.*, annually and for rejected prohibited transactions) that must be adhered to. Licenses may include additional requirements and conditions.

Exempt transactions are generally not subject to these requirements, except in certain instances there are limited reporting requirements that apply under the exemptions.

Even for non-covered or exempt transactions, it is generally a prudent best practice to maintain records for at least 10 years showing the non-applicability of the final rule (or the applicability of the exemption) to those transactions.

Conclusion

The DOJ's final rule marks a pivotal shift in U.S. data security policy. These rules apply even to activity conducted between the U.S. and third countries, and where all parties are commercial operators. They reflect concerns over foreign adversaries' access to this sensitive U.S. data through a variety of means, including compulsion and even covert action.

Where applicable, CISA's Security Requirements will be very challenging for many organizations to meet, and there are serious questions about how these regulations will work in practice for many types of companies that rely on these cross-border data flows.

It is imperative that companies carefully review their data maps and analyze their data types and flows to analyze these new federal requirements that could impact their data governance programs and critical compliance obligations.

If your organization is covered by the final rule, but you believe that full compliance by April 8 may not be possible, it is critical to engage as soon as possible with DOJ. While receiving favorable guidance or licenses will require a thoughtful approach to DOJ, the regulators have indicated that they will be amenable to working with companies that are taking these regulations seriously and implementing them as quickly as they can and to the extent possible.

If you have any questions about the DOJ final rule, PADFA, or the impact of these new data restrictions on your commercial or compliance activities, do not hesitate to contact the authors of this article for guidance.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- Sanctions + Trade Controls