COVINGTON

Department of Justice Issues Final Rule to Implement Bulk U.S. Sensitive Personal Data and Government-Related Data Executive Order

ALERT

JANUARY 6, 2025

Introduction

On December 27, 2024, the U.S. Department of Justice ("DOJ") issued the **Final Rule** implementing President Biden's February 28, 2024 Executive Order on "**Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern**" (the "EO"). The Final Rule solidifies a new national security regulatory regime focused on protecting bulk U.S. sensitive personal data and government-related data from countries of concern, including the People's Republic of China ("PRC" or "China"), and represents the latest step in the U.S. government's whole-of-government effort to "de-risk" with respect to China. The Final Rule marks the first time that U.S. persons will be categorically prohibited from engaging in certain transactions that may result in foreign access to bulk U.S. sensitive personal data and government-related data. It also provides that certain other transactions will be "restricted," meaning they are prohibited unless the U.S. business first implements a range of security requirements, which in some cases will be onerous or costly. The Final Rule accordingly could have wide-ranging implications for U.S. companies across various industries. The Final Rule takes effect 90 days after publication in the Federal Register, which is set for January 8, 2025, although certain compliance requirements will not take effect until 270 days following publication.

In parallel with the release of the Final Rule, on January 3, 2025, the U.S. Cybersecurity and Infrastructure Security Agency ("CISA"), which is part of the U.S. Department of Homeland Security ("DHS"), released the final **security requirements** (the "Security Requirements"). The Security Requirements set forth the measures that U.S. persons must satisfy in order to engage in restricted transactions, and are incorporated by reference into the Final Rule.

Importantly, as we discussed in our **analysis** of the Advance Notice of Proposed Rulemaking ("ANPRM") and our **analysis** of the Notice of Proposed Rulemaking ("NPRM"), the Final Rule is a national security regulation designed to address identified risks to U.S. national security—not a privacy regulation designed to protect privacy or other individual interests. Consequently, while the Final Rule regulates transactions involving personal data, many of the concepts and definitions diverge materially from those in existing privacy regimes. The Final Rule stems from the U.S. government's increasing unwillingness to tolerate foreign adversary access to U.S. personal data. As DOJ explained in the preamble to

the Final Rule, "[t]his rule will prevent . . . foreign adversaries from legally obtaining [bulk U.S. sensitive personal data or government-related data] through commercial transactions with U.S. persons, thereby stemming data flows and directly addressing the national security risks identified in the [EO]." DOJ cited examples such as (1) the ability of journalists to track the movements of U.S. President Joe Biden, U.S. Vice President Kamala Harris, and now President-Elect Donald Trump through their bodyguards' use of a fitness app; and (2) the ability to track U.S. government personnel movement through the purchase of location information and digital advertising data—that demonstrate the U.S. national security risks associated with foreign adversary access to commercially available data. Finally, DOJ made a particular point of explaining that certain data that is anonymized or depersonalized presents U.S. national security risks, especially with respect to the ability of adversaries to use "bulk human genomic data[] to enhance military capabilities that include facilitating the development of bioweapons."

These concerns are not new but instead have been steadily growing over the past decade or more. Indeed, dating back to 2016, we have seen the Committee on Foreign Investment in the United States ("CFIUS") seek to mitigate heavily or even recommend prohibition of transactions involving U.S. companies with significant volumes of personal data and where CFIUS identified a potential risk of Chinese access to such data. However, case-by-case reviews, such as through the CFIUS process, have been viewed as insufficient to address the ever-growing national security risk and, accordingly, there has been an effort in recent years to establish a stand-alone regime to regulate certain data transactions to address national security risk. The Final Rule represents the culmination of those efforts.

The Final Rule either prohibits or restricts certain categories of transactions—data brokerage (which is defined broadly), vendor agreements, employment agreements, and investment agreements—that could result in access to certain bulk U.S. sensitive personal data or government-related data by a country of concern or covered person. Any person who violates, attempts to violate, conspires to violate, or aids or abets in commission of a violation of the Final Rule could be subject to civil and criminal penalties. This means that U.S. entities, irrespective of industry, will need to evaluate whether affiliates, partners, vendors, employees, potential investors, and commercial counterparties generally, could meet the definition of "covered person" under the Final Rule such that the regulations are implicated. For example, if a small U.S. startup company that stores bulk U.S. sensitive personal data engages in a fundraising round, it will need to evaluate whether any of the investors are "covered persons" such that the investment may be restricted. Large multinational companies will need to evaluate whether databases hosting U.S. sensitive personal data in the United States are accessible to third-party vendors or even affiliates pursuant to agreements that could implicate the Final Rule's prohibitions or restrictions. And life sciences companies may be restricted or prohibited from sharing certain U.S. clinical trial data with regulators and research partners in countries of concern unless one of the Final Rule's exemptions applies.

While it is clear that the Final Rule is broad in scope and application, we anticipate that in certain circumstances U.S. companies will face challenges in assessing what activities may be prohibited or restricted, what activities may be exempt, and what activities may be implicated or not. The Final Rule was released less than two months after the publication of the **NPRM**, and only four weeks after public comments on the NPRM were due. Perhaps due to this aggressive timeline, certain aspects of the rule remain unclear or ambiguous. Several commenters to the NPRM focused on the need for further clarification with respect to various aspects of the regulations, including, for example, the intended reach of the "data brokerage" definition and the scope of activities covered by certain of the exemptions. While certain changes were made to the text of the Final Rule—including with respect to certain of the exemptions that will apply to transactions that would otherwise be in scope—the Final Rule largely tracks the language of the NPRM and leaves some important comments unaddressed. DOJ appeared to acknowledge these issues by emphasizing that it anticipates providing additional guidance in the coming weeks and months, and noting that regulated entities should engage both informally as well as through the Final Rule's advisory opinion process to seek additional clarity on a case-by-case or even industry-wide basis.

Discussion of the Final Rule

Overview

The overall structure of the Final Rule is broadly unchanged from the NPRM and will either outright prohibit, or otherwise restrict, certain transactions that involve access to bulk U.S. sensitive personal data or government-related data. Specifically, as directed by the EO, the Final Rule regulates **covered data transactions**—which the Final Rule defines as "any transaction that involves any access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data and that involves: (1) Data brokerage; (2) A vendor agreement; (3) An employment agreement; or (4) An investment agreement." But for one exception described below, the prohibitions and restrictions apply only when those covered data transactions are between a U.S. person and a **country of concern** or **covered person**. The Final Rule also includes a number of exemptions, such as certain transactions related to personal communications, telecommunications services, corporate group transactions, financial services, and life sciences.

Countries of Concern and Covered Persons

The list of countries of concern in the Final Rule remains the same as the NPRM: China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela. However, the definition of the term "covered person" is slightly changed from the NPRM. These changes by DOJ were intended to ensure the definition of "covered person" conforms with the originally intended scope of the term, and to ensure the definition is consistent with the Department of the Treasury's Office of Foreign Assets Control's ("OFAC") "50-percent rule language." The Final Rule's definition of covered person is:

1. A foreign person that is an entity that is 50 percent or more owned, directly or indirectly, individually or in the aggregate, by one or more countries of concern or persons described in paragraph (2) below; or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern;
2. A foreign person that is an entity that is 50 percent or more owned, directly or indirectly, individually or in the aggregate, by one or more persons described in paragraphs (1) above or (3), (4), or (5) below;
3. A foreign person that is an individual who is an employee or contractor of a country of concern or of an entity described in paragraphs (1) or (2) above, or (5) below;
4. A foreign person that is an individual who is primarily a resident in the territorial jurisdiction of a country of concern; or
5. Any person, wherever located, determined by the Attorney General: (i) To be, to have been, or to be likely to become owned or controlled by or subject to the jurisdiction or direction of a country of concern or covered person; (ii) To act, to have acted or purported to act, or to be likely to act for or on behalf of a country of concern or covered person; or (iii) To have knowingly caused or directed, or to be likely to knowingly cause or direct a violation of the Final Rule.

Thus, the Final Rule's definition of covered person extends not only to, for example, Chinese subsidiaries of non-Chinese companies, but also to any entity that is 50 percent or more owned by a Chinese party, any foreign person who is an employee of such entity, or any foreign person who is primarily resident in China. Further, the Final Rule clarifies that at least two levels of ownership must be reviewed to determine if an entity is a covered person. For instance, if a covered person owns 50 percent of Entity A, and Entity A in turn owns 50 percent of Entity B, Entity B would be considered a covered person. Moreover, the Final Rule makes clear that foreign ownership can also be satisfied in the aggregate. Thus, if in the previously discussed example, Entity A only owns 40 percent of Entity B, but Entity C, which is also a covered person, owns 10 percent of Entity B, the total covered person ownership would be 50 percent, satisfying the Final Rule's definition of covered person.

Consistent with the NPRM, nationals of any country of concern located in the United States will be treated as U.S. persons—not covered persons—unless otherwise designated by the Attorney General. Similarly, a U.S. entity solely organized under the laws of the United States—even if ultimately owned or controlled by a covered person—will be considered a U.S. person unless designated otherwise.

Finally, it is important to note that in the preamble, DOJ advised U.S. persons to exercise caution when engaging in transactions with entities that are not covered persons, "but in which one or more covered persons have significant ownership that is less than 50 percent, or which one or more covered person may control by means other than a majority ownership interest." DOJ noted that such entities' ownership structure may fluctuate over time causing it to become a covered person, or the entity could be designated a covered person by DOJ.

Covered Data

Two different categories of data are regulated by the Final Rule: **bulk U.S. sensitive personal data** and **government-related data**.

U.S. sensitive personal data is defined as "covered personal identifiers, precise geolocation data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof." It does not include public or nonpublic data not related to an individual, or data lawfully available to the public from a government record or in "widely distributed media."

U.S. sensitive personal data is regulated at the corresponding "bulk" thresholds, with "bulk" defined as any amount of sensitive personal data that meets or exceeds the following thresholds at any point in the preceding 12 months, whether through a single transaction or aggregated across transactions "involving the same U.S. person and the same foreign person or covered person":

Data Category	Bulk Threshold
Human 'omic data	More than 1,000 U.S. persons (but for human genomic data, the threshold is more than 100 U.S. persons)
Biometric identifiers	More than 1,000 U.S. persons
Precise geolocation data (i.e., within 1,000 meters)	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
Covered personal identifiers	More than 100,000 U.S. persons
Combined data–meaning any collection or set of data that contains more than one of the categories above, or that contains any listed identifier linked to the categories above excluding covered personal identifiers, 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.	

One notable change in the Final Rule, as previewed in the preamble to the NPRM, is that the focus on human genomic data was expanded to human 'omic data—which consists of human epigenomic data, human proteomic data, and human transcriptomic data, in addition to human genomic data. DOJ indicated in the preamble to the NPRM that it was considering including nine other categories of human 'omic data in the Final Rule (after stating in the ANPRM only human genomic data was being contemplated for inclusion as part of this initial round of rulemaking to implement the EO), but reasoned in the preamble to the Final Rule that these three other human 'omic fields merit inclusion because they are the "most advanced" and have the greatest clinical and predictive capacity. The Final Rule defines the three new human 'omic data categories to exclude certain "routine clinical measurements" for "individualized patient care purposes" (although such data likely constitutes personal health data under the Final Rule). Further, the Final Rule expressly excludes "pathogen-specific data embedded in 'omic data sets" from the scope of all four human 'omic data categories.

Government-related data is defined to include "[a]ny precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List" or "[a]ny 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], including the military and Intelligence Community." Notably, as the definition includes precise geolocation related to the list of government-related locations, U.S. companies will need to assess whether they collect *any* data from such locations for purposes of assessing applicability of the Final Rule. Moreover, the list of government-related locations expanded from eight locations in the NPRM to 736 locations in the Final Rule.

Prohibited and Restricted Transactions

Prohibited transactions are the following covered data transactions undertaken by a U.S. person:

- Any covered data transaction involving data brokerage with a covered person or a country of concern. Importantly, the term "data brokerage" is broadly defined as "the sale of data, licensing of access to data, or similar commercial transactions . . . 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." It encompasses a range of transactions that many businesses may not consider "brokering" transactions in the traditional commercial sense. While DOJ did make clear that data brokerage excludes the commercial transactions of employment, vendor, and investment agreements, DOJ declined to further clarify the definition or limit the breadth of the term.

  In the preamble, DOJ stated that covered data transactions require some form of a "commercial nexus," including consideration. However, the discussion of what constitutes "consideration" introduced its own ambiguity. For instance, DOJ noted that sharing data for the purposes of a mutual interest in co-authoring a paper for submission to an academic journal, by itself, would be insufficient to constitute valuable consideration. By contrast, DOJ noted in the discussion of employment agreements that "unpaid service on a volunteer board" could constitute "other consideration," as there is a "value and benefit derived from one's experience."

  DOJ also added additional examples of what may constitute "data brokerage," which illustrate that the term is intended to reach well beyond the traditional understanding of data brokerage. One example states that if a U.S. company owns or operates a mobile app that contains one or more tracking pixels or software development kits ("SDKs") that were knowingly installed or approved for incorporation into the mobile app by the U.S. company, and those tracking pixels or SDKs transfer or otherwise provide access to bulk U.S. sensitive personal data to a covered person-owned social media app for targeted advertising, such transaction would be prohibited. Another example states that where a U.S. researcher receives a grant from a university in a country of concern to study bulk personal health data and bulk human 'omic data on U.S. persons, and the grant directs the researcher to share the underlying bulk U.S. sensitive personal data with the university, the transaction is prohibited data brokerage "because it involves the transfer of bulk U.S. sensitive personal data to a covered person in return for a financial benefit."

- Any covered data transaction that involves access by a covered person to bulk U.S. human 'omic data, or to human biospecimens from which bulk human 'omic data could be derived. As noted above, this is an expansion of the NPRM, which included only bulk human genomic data and did not include other categories of human 'omic data.
- A covered data transaction involving data brokerage with any foreign person that is not a covered person, unless the U.S. person imposes contractual commitments on the foreign person not to engage in a subsequent transaction involving that data with a country of concern or covered person.
- A transaction "that has the purpose of evading or avoiding, causes a violation of, or attempts to violate" the Final Rule's prohibitions. Conspiracy to violate the requirements of the Final Rule is also expressly prohibited.
- "Knowingly directing prohibited or restricted transactions" (unless the restricted transaction complies with the Final Rule's requirements).

Restricted transactions are any covered data transactions involving a vendor agreement, employment agreement, or investment agreement with a country of concern or covered person, and are prohibited unless the U.S. person party to the transaction adopts compliance measures specified by the Final Rule, including the Security Requirements incorporated by reference.

The definitions of vendor, employment, and investment agreements remain largely unchanged from the NPRM but for one change made to the investment agreement exclusions. Specifically, in the NPRM, DOJ carved out from the definition of "investment agreement" any investment that:

1. Is made (i) into a publicly traded security, (ii) into a security offered by an investment company or company regulated as a business development company; or (iii) as a limited partner in a venture capital fund, private equity fund, fund of funds, or other pooled investment fund, so long as that limited partner is strictly passive;
2. Gives the covered person less than 10 percent in total voting and equity interest; **and**
3. Does not give a covered person rights beyond those reasonably considered to be standard minority shareholder protections.

In response to this exclusion, at least one commenter suggested that it should extend not only to investments in public companies, but also "one-percent, passive, minority investments into private U.S. entities" (i.e., companies whose shares are not traded publicly), as the investment will additionally need to satisfy prong (3) of the exclusion, and therefore would be "passive." DOJ wrote in the preamble that it "agreed" with the commenter, but then in the Final Rule, rather than expanding the exclusion to apply to direct investments in private entities that otherwise meet the exclusion criteria, DOJ instead only expanded the exclusion to exclude investments "as a limited partner . . . in a private entity." This language is confusing because investments as a limited partner are, by definition, only made into limited partnerships—not other types of "private" corporate entities such as corporations and limited liability companies whose shares are not publicly traded. This suggests that the "expansion" of the exclusion for passive investments applies only in the rare instance that a minority investment is made directly into a limited partnership that has U.S. sensitive personal data or government-related data (as opposed to indirectly through a limited partnership into an operating company holding such data, which is already separately excluded in the exclusion for passive investments). The policy rationale for limiting the exclusion in this respect is unclear to us, and we wonder whether this was indeed DOJ's intent.

The narrow exclusion for passive investments also creates ambiguity as to whether <u>all</u> investments by covered persons into U.S. entities that collect bulk U.S. personal data will be considered "covered data transactions" (i.e., a transaction that would involve *access* to bulk U.S. sensitive personal data or government-related data). On the one hand, it would be a stretch for DOJ to take the position that a one percent, passive investment in a privately-held company necessarily involves "access" to bulk U.S. sensitive personal data and therefore is a "restricted transaction," especially if the company and the investor expressly agree that the investor will have no access to such data and no such assess is in fact provided. Further, in one example the Final Rule appears to equate "access" with non-passive investments, where it explains that an investment agreement that affords a covered person a minority equity stake in a U.S. business that collects bulk U.S. sensitive personal data would be restricted even where the agreement explicitly forbids the covered

person from accessing the U.S. data*, if the agreement nonetheless affords the covered person* "*sufficient ownership interest, rights, or other involvement in substantive business decisions, management, or strategy such that the investment does not constitute a passive investment*" (emphasis added). On the other hand, the Final Rule does not define "passive investment"; the closest language to such a definition is the "exclusion for passive investments" as described above—which suggests DOJ may take the position that unless an investment meets the criteria contained in the exclusion, it will view an investment as non-passive. This appears to be a material area of inconsistency or ambiguity in the Final Rule that is ripe for clarification, especially considering the wide-ranging implications for venture investments.

Compliance Requirements

The Final Rule largely adopts the compliance requirements described in the NPRM, with a few notable changes described in more detail below. In the preamble to the Final Rule, DOJ noted several times that it appreciated there would be compliance costs associated with the Final Rule, and it extended the effective date for many of the Final Rule's compliance provisions to 270 days after the Final Rule is published in the Federal Register in recognition of those costs. However, DOJ also described its view that many regulated parties should be able to leverage existing compliance programs to also meet their obligations under the Final Rule, given the overlap between the Final Rule and "the existing compliance expectations set by other regulators, such as [OFAC] and the Department of Commerce's Bureau of Industry and Security ("BIS"), for screening vendors and transaction counterparties."

Restricted Transaction Requirements

As a condition to engage in a restricted transaction, a U.S. person must (1) comply with the CISA Security Requirements; (2) implement a data compliance program, described in a written policy; and (3) conduct annual audits.

Audits

The Final Rule requires an annual audit by any U.S. person who engages in any restricted transaction. As compared to the NPRM, the Final Rule removes the requirement for audits to be conducted by an external auditor. The Final Rule only requires that the auditor must be "independent." Furthermore, the Final Rule clarifies that the scope of the audit is limited to the "U.S. person's restricted transactions" and is to be focused on "relevant" material (e.g., policies, personnel, and facilities).

Recordkeeping

The Final Rule requires that U.S. persons engaged in any transaction subject to the Final Rule prepare and maintain records of each such transaction for at least 10 years after the date of the transaction. Additionally, as under the NPRM, the Final Rule requires U.S. persons engaged in any restricted transaction to also maintain the following records:

- A written policy that describes the data compliance program;
- A written policy that describes the implementation of the applicable security requirements (described below);
- The results of annual audits to verify compliance with security requirements and any conditions on a license;
- Documentation of due diligence to verify the data flow of restricted transactions which incorporates:
    - The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;
    - The identity of the transaction parties;
    - A description of the end-use of the data; and

- Documentation and copies of related information including method of data transfer, date of transaction, agreements associated with the transaction, relevant licenses and advisory opinions, and annual certification of the accuracy and completeness of the records.

Reporting

The Final Rule retains the same authority proposed in the NPRM for DOJ to require a report on demand related to "any act or transaction or covered data transaction . . . subject to the provisions" of the Final Rule. In addition, any U.S. person that has received and rejected (including automatically through use of software or other digital tools) an offer from another person to engage in a prohibited data brokerage transaction must submit a report within 14 days of rejecting such transaction. Moreover, as proposed by the NPRM, U.S. persons engaged in restricted transactions involving cloud-computing services are required to submit annual reports where 25 percent or more of that U.S. person's equity interests are owned by a country of concern or covered person. DOJ did not clarify directly in the Final Rule what is meant by transactions "involving cloud-computing services," though DOJ did explain that the rationale for the annual reporting requirement is to provide DOJ with "information about companies with notable country of concern ownership that access large amounts of sensitive personal data," presumably because they *provide* cloud-computing services, rather than *use* a third-party cloud service provider.

Exemptions

As discussed in the NPRM, the Final Rule provides a number of exemptions:

- Personal communications;
- Information or informational materials;
- Travel;
- Official business of the U.S. government;
- Transactions "ordinarily incident to and part of the provision of financial services";
- Corporate group transactions;
- "Transactions required or authorized by Federal law or international agreements, or necessary for compliance with Federal law";
- Investment agreements subject to a CFIUS action";
- Transactions "ordinarily incident to and part of the provision of telecommunications services";
- "Drug, biological product, and medical device authorizations"; and
- "Other clinical investigations and post-marketing surveillance data."

Several of these exemptions include notable changes or clarifications from the NPRM, which are discussed in further detail below.

Financial Services

The Final Rule exempts data transactions to the extent that they are "ordinarily incident to and part of the provision of financial services" which includes, but is not limited to, banking, capital markets, financial activity authorized by national banks, an activity that is "financial in nature or incidental to such financial activity" as set forth in the Bank Holding Company Act, the transfer of financial data or personal identifiers in connection with the sale of goods and services, the

processing of payments or fund transfers, and the provision of investment-management services. In the preamble to the Final Rule, DOJ addressed the breadth of this exemption, noting that the "exemption is not only applicable to the activities of financial institutions [as one of the Final Rule's] example[s] shows that the exemption can apply to a U.S. company operating an online marketplace." In other words, the exemption is focused on activities of a U.S. company rather than the industry in which the U.S. company operates. While broad, the Final Rule also makes clear that the financial services exemption has certain limits. As previewed in the NPRM, DOJ retained two examples that indicate the limits of the exemption:

- In Example 4, the Final Rule states that the use of a covered person in a country of concern to provide data storage services, if the data stored is data related to "payments . . . between U.S. persons in the United States and do not involve a country of concern," is not an exempted transaction. The Final Rule states that such a transaction "is not ordinarily incident to facilitating" such payments.
- In Example 12, the Final Rule states that the appointment of a covered person to the board of directors of a U.S. company that provides wealth-management services, where the covered person "could compel company personnel or influence company policies or practices to provide the director access to the underlying bulk personal financial data the company collects on its U.S. clients" would not constitute an exempted transaction. DOJ's position is that "[t]he board member's access to the bulk personal financial data is not ordinarily incident to the U.S. company's provision of wealth-management services."

Finally, in response to comments asking that DOJ clarify that the exemption would extend to the development of products —which DOJ understood to be fraud and detection prevention models—DOJ stated that it declined to "extend the exemption to product development" as it was not clear to DOJ why bulk U.S. sensitive personal data needs to be accessed in a country of concern or by a covered person to develop such products as part of providing financial services.

Corporate Group Transactions

The prohibitions and restrictions in the Final Rule will also not apply to data transactions to the extent they are (1) between a U.S. person and its subsidiary or affiliate located in (or otherwise subject to the ownership, jurisdiction, or control of) a country of concern; and (2) ordinarily incident to and part of administration of ancillary business including human resources, corporate financial activities such as payroll, paying business fees or taxes, obtaining business licenses or permits, sharing data with auditors and law firms for regulatory compliance, risk management, business-related travel, customer support, employee benefits, and employees' internal and external communications.

DOJ's discussion of this exemption offered additional insight into the scope (and limitations) of how the exemption will be interpreted and applied. First, DOJ emphasized that "core business activities" are not covered under the exemption, which includes product research and development. Second, DOJ indicated that where a foreign subsidiary that is a covered person provides customer support to U.S. customers, and where part of that support includes accessing bulk U.S. sensitive personal data, that such access may not be considered "ordinarily incident to and part of the provision of customer support"; DOJ implied if the support is provided "in all instances—including instances in which customer support is being provided to U.S. persons located in the United States—and not just in instances that involve a country of concern or a covered person" that such support would not be covered under the exemption. On the other hand, DOJ also stated that the list of activities contained within the exemption is not exhaustive, and moreover that additional guidance would be provided by DOJ in the coming weeks and months regarding what may or may not be considered in scope for this exemption.

Life Sciences

The life sciences exemptions in the Final Rule have also been expanded and clarified. First, the Final Rule adopts a de-identification/pseudonymization standard (consistent with the standard for U.S. Food and Drug Administration's ("FDA's") post-marketing adverse event reporting in 21 C.F.R. 314.80(i)) for the exemption pertaining to drug, biological product,

and medical device authorizations ("Regulatory Authorization Exemption"), and the exemption pertaining to other clinical investigations and post-marketing surveillance ("U.S. FDA Submission Exemption"). Second, for the Regulatory Authorization Exemption, the exemption has been expanded to include transactions of regulatory approval data that are "required by the regulatory entity to be submitted to a covered person to obtain or maintain authorization or approval," such as a local registered agent, a laboratory, or an Ethics Committee. By contrast, the transfer of covered data to a vendor for storage and organizational purposes, if not necessary to obtain regulatory approval, would not constitute an exempt transaction. Third, DOJ clarified that the Regulatory Authorization Exemption "is not limited to circumstances in which the data is necessary for the *U.S. person* to obtain or maintain regulatory authorization or approval to market a drug . . ." (emphasis added). Thus, U.S. entity data-sharing with entities in a country of concern that are themselves seeking to obtain regulatory approval could fall within the exemption. Fourth, DOJ revised the Regulatory Authorization Exemption to ensure it covers the provision of regulatory approval data to covered persons to obtain regulatory approval in a foreign country that is not a country of concern. Finally, DOJ agreed that covered data transactions in the context of regulatory inspections generally would fall within the Regulatory Authorization Exemption, provided the inspection is necessary to obtain or maintain regulatory authorization, but "the release of unredacted, identifiable bulk U.S. sensitive personal data . . . would generally fall outside the scope of the exemption, even when accessed as part of a regulatory inspection." DOJ is continuing to evaluate whether a broader exemption for regulatory inspections is warranted, including the appropriateness of a general license.

DOJ confirmed that the U.S. FDA Submission Exemption applies only to U.S. FDA-regulated activities. This means that local clinical trials conducted in a country of concern to support an application for regulatory approval in the country of concern are not exempt, though in many instances such transactions could proceed as restricted transactions. DOJ also made clear that the Regulatory Authorization Exemption and the U.S. FDA Submission Exemption do not extend to dietary supplements and other "health foods," nor to cosmetics.

Telecommunications Service

In addition to the above, the Final Rule, like the NPRM, exempts "data transactions, other than those involving data brokerage, to the extent that they are ordinarily incident to and part of the provision of telecommunications services." Of note, the telecommunications service exemption was expanded to incorporate more modern technology, and now covers "the provision of voice and data communications services regardless of format or mode of delivery, including communications services delivered over cable, Internet Protocol" and other methods.

Licensing

The Final Rule adopts the licensing framework initially described in the NPRM, which DOJ explained in connection with the NPRM would allow for the issuance of licenses "only in rare circumstances as the Attorney General deems appropriate." At the same time, DOJ also pointed to the licensing scheme several times throughout the preamble to the Final Rule as an option where DOJ declined to expand or adopt an additional exemption, or otherwise did not substantively address a commenter's request.

The Final Rule provides a process for DOJ to issue both general and specific licenses. Any person that has an interest in a transaction or proposed transaction may apply for a specific license for that transaction. The application must describe with specificity the transaction, the parties involved, and the end-use and method of data transfer involved. DOJ will endeavor, but is not required, to respond to any specific license request within 45 days of having received the application and any additional information requested by DOJ. If granted, and unless otherwise specified, a specific license applies only between the parties identified in the license, only with respect to the data described in the license, and only to the extent the conditions specified in the license are satisfied. DOJ indicated that in some cases, however, a specific license may apply to more than one transaction, such that companies will not have to seek licenses for each data transfer presumably involving the same parties and the same or similar data. DOJ may, at its discretion, issue general licenses

that apply more broadly, such as where multiple companies in the same industry request specific licenses on the same topic. General licenses will be published in the Federal Register.

While licenses will primarily cover otherwise *prohibited* transactions, DOJ retained the discretion to issue licenses with respect to otherwise *restricted* transactions, which would function to relieve parties of some or all of the Security Requirements associated with such transactions. In connection with any specific license issued by DOJ, the Final Rule allows DOJ to impose additional requirements on parties on a case-by-case basis. DOJ may also condition general licenses on compliance with additional requirements.

Advisory Opinions

Consistent with the NPRM, the Final Rule provides that any U.S. person party to a transaction potentially subject to the Final Rule may request a statement from the Attorney General of DOJ's "present enforcement intentions" with respect to the transaction. Advisory opinion requests must be submitted by a U.S. person party to the transaction (or its agent—which could include a trade association as discussed in the NPRM), and apply only to the party or parties to the request. To receive an advisory opinion, the U.S. person must specify the actual nature of the transaction (which includes the prospective conduct with respect to which the opinion is sought) and the specific parties involved, rather than posing a hypothetical. In response to an advisory opinion request, DOJ may state its present enforcement intention with respect to the transaction, may decline to do so, or may take "such other position or initiate such other action as it considers appropriate." DOJ will endeavor, but is not required, to respond to any request within 30 days. Parties to the request may rely on any advisory opinion issued by DOJ with respect to the transaction, but, importantly, no other agency is bound by the opinion, nor is DOJ prohibited from taking action under other statutory or regulatory authorities.

DOJ indicated that it intends to make any official guidance generated through the advisory opinion process publicly available to help parties better understand the regulations, in addition to publishing the advisory opinions themselves. Indeed, in its discussion of comments on the NPRM, DOJ pointed to the advisory opinion process in several places as a means of addressing continuing ambiguity in various provisions of the Final Rule.

"Knowingly" Standard and Safe Harbor

The Final Rule maintained the "knowingly" liability standard contemplated in the NPRM—which the Final Rule defines as either the person's "actual knowledge, or [what the person] reasonably should have known." The Final Rule includes the same example from the NPRM that if a provider "specializes" in providing cloud storage for human genetics companies, then by virtue of being specialized, the provider should know that its customers' data is likely sensitive personal data (e.g., human genomic data). Thus, if the cloud provider hires IT personnel in a country of concern—i.e., enters into an employee agreement with a covered person—then the cloud-service provider may have knowingly engaged in a prohibited transaction. However, as the discussion in the NPRM stated, if in the ordinary course of business a provider does not access customer data and has no reason to know the customer is engaged in covered data transactions, the provider would not be subject to the requirements of the (then Proposed) Rule because they would not know, or have reason to have known, the nature of the customer's data and transactions.

Moreover, in the Final Rule, DOJ declined to create a safe harbor for due diligence practices, but recognized that such a provision could be included in the future. DOJ further noted that it will consider "license applications and requests for advisory opinions" on such issues once the Final Rule is effective.

Additional Notable Considerations

Evasions or Violations via Artificial Intelligence

The Final Rule maintains the prohibition on evasions through artificial intelligence ("AI"). While DOJ did not expressly restrict the licensing of AI models through the regulations, the Final Rule states that if a transaction is structured for purposes of evading these regulations—i.e., the covered person licenses a model for purposes of accessing the U.S. sensitive personal data—such transaction would be a violation of the regulations. This could include, for example, a transaction that gives a country of concern or covered person access to an AI model trained on bulk U.S. sensitive personal data and where the receiving party could feasibly access the underlying data by querying the model to share some or all of the data.

However, DOJ clarified in the preamble that "mere access to an algorithm that was trained on bulk U.S. sensitive personal data, by itself, [does not] constitute access to the underlying data." It further emphasized this point by the reiteration of the "knowingly" standard in one of the examples in the Final Rule, which states that if the company "*kn[ew]* that the algorithm can reveal the training data" (emphasis added) that included bulk covered personal identifiers, then "licens[ing] the derivative algorithm . . . for the purpose of accessing bulk sensitive personal identifiers from the training data" would be prohibited.

Enforcement and Penalties

The Final Rule tracks the NPRM with respect to enforcement and penalties, allowing for the imposition of both civil and criminal penalties in the event of a violation (in addition to a "finding of violation" with respect to which no penalty is imposed). Civil penalties, per violation, cannot exceed the greater of $368,136 or an amount that is twice the amount of the transaction that is the basis of the violation. For any person who willfully commits, attempts to commit, conspires to commit, or aids or abets in the commission of a violation of the Final Rule, criminal penalties, per violation, cannot exceed a fine of $1,000,000, imprisonment of 20 years, or both.

In connection with penalties, the Final Rule maintains the proposed pre-penalty notice process, whereby DOJ will issue a written notice informing the alleged violator of DOJ's intent to impose a penalty. The alleged violator has the right to respond to such a notice, after which DOJ may determine that a finding of violation is not warranted or to impose a penalty. DOJ's issuance of a penalty notice is subject to judicial review in Federal district court as a final agency action. In response to a comment on the NPRM, DOJ indicated that it will publish compliance and enforcement guidance to help parties comply with the Final Rule, including with respect to how DOJ will assess voluntary self-disclosures.

Applicability

The Final Rule offered further insight into the applicability of the provisions. First, DOJ stated in the preamble that "[t]he [Final R]ule applies to covered data transactions engaged [in] on or after the effective date"; it does not apply retroactively. However, DOJ indicated in the preamble that the "covered data transaction" is not the contract or other instrument that represents the anticipated transaction, but is in fact a reference to the actual transfer. Therefore, if an individual enters a contract for data brokerage prior to the Final Rule's effective date, any transactions prior to the effective date would not be prohibited, but any transactions that occur under the contract *after* the Final Rule's effective date would fall under the Final Rule's authority and could thus be prohibited or restricted.

Second, while the majority of the Final Rule's provisions will go into effect 90 days after the publishing of the Final Rule in the Federal Register, there are several provisions which will not go into effect until 270 days after the publication of the Final Rule:

- The "due diligence and audit requirements for restricted transactions";
- The requirement to file an annual report for engaging in certain cloud computing-related restricted transactions; and
- The obligation to report if a U.S. person "has received and affirmatively rejected" an offer "to engage in a prohibited transaction involving data brokerage."

Though DOJ declined to extend the effective date in response to comments on the NPRM, DOJ indicated that during the phase-in period prior to the effective dates, it will continue to engage with stakeholders to determine whether additional time for companies to come into compliance should be granted, for example by delaying the effective date, or by issuing general licenses or a non-enforcement policy for a specified period, or with respect to certain sectors, activities, or compliance requirements.

Finally, it bears emphasizing that the obligations put in place by this national security regime are primarily the obligations of U.S. persons. However, the effect of the regulations will be to limit the ability of covered persons (and countries of concern) to engage in covered data transactions and U.S. persons must report rejected prohibited transactions to DOJ. As a result, non-U.S. companies should remain apprised of the requirements of the Final Rule, as they may inadvertently find themselves on the other end of reports that U.S. entities are obligated to file within 14 days of rejecting such transactions.

Security Requirements

The CISA Security Requirements, which CISA issued on January 3, 2025, are incorporated by reference in the Final Rule and include organizational-, system-, and data-level requirements that are largely adapted from (and cross reference) the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, NIST Privacy Framework, and CISA's Cross-Sector Cybersecurity Performance Goals.

CISA's Security Requirements include two categories of requirements:

- Organizational- and system-level requirements, which cover documentation and policy requirements, logical and physical access controls, and data risk assessments. This includes, for example:
  - Designating an individual (e.g., a Chief Information Security Officer) responsible for cybersecurity and governance, risk, and compliance functions;
  - Remediating known vulnerabilities "within a risk-informed span of time";
  - "[M]aintain[ing] an accurate network topology of the covered system and, to the extent technically feasible, any network interfacing with a covered system";
  - "[I]mplement[ing] an administrative policy that requires approval before new hardware or software is deployed in/on a covered system";
  - Implementing logical and physical access controls to prevent covered persons or countries of concern from gaining access to covered data; and
  - Conducting internal data risk assessments to evaluate the sufficiency of data-level requirements, described below.
- Data-level requirements, such as data minimization and data masking, encryption, privacy enhancing technologies, and identity and access management. This includes, for example:
  - "Apply[ing] data minimization and data masking strategies";
  - "Apply[ing] encryption techniques to protect covered data during the course of restricted transactions," including comprehensive encryption during transit and storage and cryptographic key management; and
  - l"Apply[ing] privacy enhancing technologies, such as privacy preserving computation . . . or differential privacy techniques . . . , to process covered data."

CISA made several notable changes to the final Security Requirements. Critically, CISA incorporated edits clarifying that access to "covered data" is permitted during restricted transactions when the U.S. person complies with the Security Requirements and "the combination of security mechanisms deployed fully and effectively prevents access to covered data that is *linkable, identifiable, unencrypted, or decryptable* using commonly available technology by covered persons and/or countries of concern" (emphasis added). In line with CISA's clarifying edits to the Security Requirements, DOJ stated in the preamble to the Final Rule that if "a sufficient combination of" the Security Requirements are applied such that access is only provided "to an appropriately mitigated version of the data or" if access is directly denied, the transaction may proceed as a restricted transaction. This enables the Final Rule to "promote[] effective methods while prohibiting ineffective methods." However, DOJ's discussion in the preamble of the Final Rule also indicated recognition that there may be circumstances under which compliance with the Security Requirements for purposes of a restricted transaction may effectively constitute a prohibition on the transaction.

Further, the Security Requirements now exclude certain information systems from the definition of "covered system," noting that covered system "does not include an information system . . . that has the ability to view or read sensitive personal data . . . but does not ordinarily interact with such data in bulk form." However, CISA carved out from this exclusion systems that can view or read *government-related data*. This falls in line with the Final Rule's general lower tolerance for access to government-related data, where *any* quantity of government-related data constitutes covered data.

Finally, CISA softened its language in a few instances, such as by allowing U.S. persons to remediate known exploitable vulnerabilities "within a risk-informed span of time," listing 45 calendar days as the outer-most limit, versus the previously proposed 14 calendar days, and removing altogether the time limits to respond to vulnerabilities that are not known to be exploited.

Relatedly, DOJ declined to adopt generally applicable definitions or standards for the term "de-identified," "anonymized," or "pseudonymized" in the Final Rule, indicating its desire to allow the Final Rule to stay current with the passage of time. DOJ stated that "techniques evolve" and "the [F]inal [R]ule is intended to capture these developments and remain technology neutral."

If you have any questions concerning the material discussed in this client alert, please contact the members of our CFIUS practice.

Related Professionals

David N. Fagan

PARTNER

+1 202 662 5291

dfagan@cov.com

Heather L. Finstuen

PARTNER

+1 202 662 5823

hfinstuen@cov.com

Mark E. Plotkin

PARTNER

+1 202 662 5656

mplotkin@cov.com

Jonathan R. Wakely

PARTNER

+1 202 662 5387

jwakely@cov.com

Julia F. Post

OF COUNSEL

+1 202 662 5249

jpost@cov.com

Ingrid Price

SPECIAL COUNSEL

+1 202 662 5838

iprice@cov.com

Janine N. Slade

SPECIAL COUNSEL

+1 202 662 5239

jslade@cov.com

Brian S. Williams

OF COUNSEL

+1 202 662 5270

bwilliams@cov.com

Lawrence Barker

ASSOCIATE

+1 202 662 5437

lbarker@cov.com

Alexandra Bruer

ASSOCIATE

+1 202 662 5588

abruer@cov.com

Corinne Cook

ASSOCIATE

+1 202 662 5077

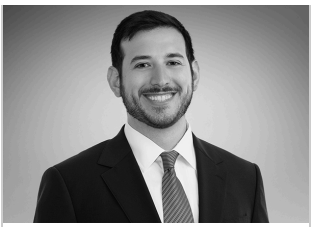
ccook@cov.com

Jacob T. Crump

ASSOCIATE

+1 202 662 5591

jcrump@cov.com



Sam Karson

ASSOCIATE

+1 202 662 5341

skarson@cov.com

Brian J. Kim

ASSOCIATE

+1 202 662 5703

bkim@cov.com

Monty Roberson

ASSOCIATE

+1 202 662 5903

mroberson@cov.com

Madeline E. Sanderford

ASSOCIATE

+1 202 662 5408

msanderford@cov.com

Related Practices

- Regulatory and Public Policy
- CFIUS

- International Trade
- Data Privacy and Cybersecurity
- Health Care
- Food, Drug, and Device
- Medical Devices and Diagnostics

Related Industries

- Life Sciences

COVINGTON