Published on *The National Law Review* https://natlawreview.com

Data, Deals, and Diplomacy, Part III: DOJ Issues National Security Final Rule with New Data Compliance Obligations for Transactions Involving Countries of Concern

Article By:

Townsend L. Bourne

Jonathan E. Meyer

Jordan Mallory

On January 8, 2025, the Department of Justice ("DOJ") published its final rule addressing Executive Order (E.O.) 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." With the final rule, the DOJ National Security Division's Foreign Investment Review Section ("FIRS") defines prohibited and restricted data transactions, and outlines trusted data flows for companies with overseas operations involving countries of concern, including IT infrastructure. The general effect of the rule is to close "front door" access to bulk sensitive personal data on U.S. persons and certain U.S.-government-related data. Until now—or rather, April 8, 2025, when the majority of the rule becomes effective—nefarious actors could procure sensitive data through legitimate business transactions.

We discussed the development of the new regulation in previous blogs (here and here), and the contours of the final rule are largely unchanged from the proposed rule. In this blog, we focus on some key clarifications and updates in the final rule. Then, we turn to what this final rule means for companies with operations in countries of concern and the questions every company with overseas IT infrastructure should be asking to know if these regulations might apply to them.

1. Updates in the Final Rule

There were no big surprises with the final rule, and it remains largely unchanged from the proposed rule. For the uninitiated, the rule prohibits or restricts a subset of *covered* transactions by U.S. persons involving *covered* data with *covered* persons.[1] The definitions of what is *covered* remain the same—even the bulk thresholds are the same as the proposed rule. However, below we highlight some of the key developments hidden among the minor clarifications and conforming edits.

1.1. Effective Date and Delayed Compliance Date. The rule sets an effective date of April 8, 2025 for every component of the rule except for specified compliance obligations. Those obligations, which

include the due diligence and audit requirements from Subpart J and the reporting and recordkeeping requirements of Subpart K, do not require implementation until October 6, 2025. Those delayed compliance obligations do not encompass the security requirements required for restricted transactions and thus cybersecurity requirements established by CISA should be in place before engaging in any restricted transaction after April 8, 2025.

1.2. Expanded Government-Related Location Data List. The final rule substantially expands the Government-Related Location Data List from the 8 locations in the proposed rule to 736 locations in the final rule. These additional locations consist of commonly known Department of Defense sites and installations, such as bases, camps, posts, stations, yards, centers, or homeport facilities for any ship, ranges, and training areas in the United States and its territories. In its discussion of this list, DOJ acknowledges that it plans to provide this list in a format that would be easy for developers to access and implement (e.g., .csv, .json).

1.3. New definition of human 'omic data. The final rule creates a new sub-definition of "human genomic data" for "human 'omic data," which includes human epigenomic data, human proteomic data, and human transcriptomic data. Those three data categories have a bulk threshold of data on more than 1,000 U.S. persons.[2] These new definitions will have an impact on clinical and predictive research, particularly those implementing AI within their research.

2. Effects of the Regulation

As Assistant Attorney General Matthew Olsen said last year, this regulation is built like sanctions and export controls and is expected to have "real teeth." Any U.S. company with operations in the identified countries of concern, particularly with overseas IT infrastructure, will need to have a conversation about whether this regulation will affect their business. Companies need to know and understand the following:

- What data the company has or collects that might constitute sensitive personal data and/or Government-related data as defined in the regulations;
- What business relationships and transactions allow access to the data;
- Who internally has access to the data; and
- What security measures are in place to protect that data.

For companies impacted by this regulation, those companies will also need to understand how this regulation operates differently from other DOJ regulations and data privacy regulations. Here, DOJ has availed itself of IEEPA penalties, and this regulation operates more like sanctions and export controls. This means the regulation is very compliance-focused as opposed to using case-by-case approaches like CFIUS or Team Telecom. While corporate compliance is a key component of DOJ strategy, as we have seen with the Civil Cyber Fraud Initiative, DOJ is not shying away from enforcement. Further, the FIRS has developed the skillset and prosecutorial experience for reviewing corporate compliance programs. All to say, companies should take the April 8 and October 6, 2025 deadlines seriously.

Finally, companies should understand how this regulation operates differently from other data-related regulations. Chiefly, this is not a privacy regulation; it is a national security regulation. For that reason, the focus is not on the collection of data, but rather on the subsequent sale and/or accessibility of that data. Also, the scope of what is covered data is more limited than what companies may come to expect with state privacy laws. Rather than capture all personally identifiable information (PII), this regulation is concerned with *sensitive* information. That is to say, information

that could be exploitable. However, because the data captured by the regulation is a national security concern, there is no consent exemption, meaning companies cannot have customers opt-out of the regulation's protection.

While the programmatic compliance requirements (i.e., due diligence, auditing, reporting and recordkeeping) are not required until Q4 of this year, the effective date, and beginning of potential enforcement, is right around the corner on April 8. Additionally, companies will still need to implement the CISA security requirements by April 8 if they intend to continue with restricted transactions. Still, companies should not delay in beginning to build out and implement their compliance programs.

FOOTNOTES

[1] For more details, see our Data, Deal, and Diplomacy, Part II blog.

[2] Human genomic data's bulk threshold remains the same at more than 100 U.S. persons.

Part one **and** part two **of this series.**

National Law Review, Volume XV, Number 29