CLIENT ALERTS & INSIGHTS

United States Looks Towards its First Cross-Border Data Transfer Regime with New Executive Order

MARCH 21, 2024

President Biden issued an Executive Order last month calling on the DOJ and relevant government agencies to tighten regulations on bulk data transfers to "countries of concern."

In late February, President Biden issued Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern". The executive order calls on the US Department of Justice and relevant federal agencies to build out requirements surrounding the transfer of specific categories of personal data to "countries of concern" that will be designated by the DOJ.

While not as expansive as other jurisdictions' forays into regulating cross-border data transfers, this marks the first substantive federal-level movement towards the US regulating the general transfer of US personal data to other countries. Importantly, the called-for regulations would only cover sensitive categories of personal data and be focused on "countries of concern" such as those countries sanctioned by the Office of Foreign Assess Control-so it is narrower than many other cross-border data transfer regimes.

Notably, the executive order expressly states that the called-for regulations should **not** affirmatively require domestic storage and processing of any categories of personal data. This narrows how extensive the regulations may end up being. But it does mark a shift at the US federal level-which has otherwise shied away from a significant push for omnibus data protection regulation.

The US has frequently been cited as lagging behind on issuing an omnibus data protection law at the federal level. Many other jurisdictions-such as Europe, Canada, China, and many others-have implemented such data protection regimes. And almost all of them address, to varying degrees, the transfer of its country's personal data to other countries.

For example, transfers of European personal data to the United States often require businesses to enter into the EU Commission's Standard Contractual Clauses (or that the business receiving the data be registered in FTC's new Data Privacy Framework). Transfers of Chinese personal data now often require businesses to implement China's versions of standard contractual clauses, or engage in complex government filings, reviews, and potentially audits.

However, the US has not engaged on similar regulations-even at the state level where there are now over 16 state omnibus data protection laws. See below for more information on some key takeaways from the new executive order.

Important Definitions

The executive order specifically focuses on the protection of sensitive personal data. Defining and categorizing "sensitive" categories of personal data has become common un both US state and

other non-US data protection laws. The base definition for "sensitive personal data", as defined under the new executive order, is initially broad and covers the following categories:

- Geolocation and related sensor data;
- Biometric identifiers;
- Human 'omic data (e.g., information generated by individuals that characterize or quantify human biological molecules or metabolic data);
- Personal health data;
- Personal financial data;
- Covered personal identifiers; and
- Any other categories defined by forthcoming DOJ regulations.

"Covered personal identifiers" could end up being the broadest category, as the executive order defines it as subject to further DOJ regulations. However, the executive order does make clear it will include specifically listed classes of personal data that "*whether in combination with each other, with other sensitive date, or with other data that is disclosed by a transacting party…and that makes the personally identifiable data exploitable by a country of concern*" that could be used to identify an individual.

After the base definition, however, the executive order narrows its scope. For example, "sensitive personal data" will **not** include demographic or contact data that is linked only to other pieces of demographic or contact data or network identifiers.

Importantly, the executive order narrows the "sensitive personal data" designation further in that the above categories are only considered "sensitive" if the applicable data could be "*exploited by a country of concern to harm United States national security if that data is linked or linkable to any identifiable United States individual or to a discrete and identifiable group of United States individuals.*"

The regulations will likely drill down into what crosses this line and what would not.

The term also **excludes** (1) data that is a matter of public record and that is lawfully and generally available to the public; (2) personal communications within the scope of the International Emergency Economic Powers Act; and (3) certain import / export informational materials as defined under the International Emergency Economic Powers Act.

Potential for New Cross-Border Data Transfer Regulations

The most critical item addressed in the executive order is that the DOJ and other relevant federal agencies are called on to issue regulations "*that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in any property in which a foreign country or national thereof has any interest (transaction), where the transaction*" that:

- involves bulk sensitive personal data or U.S. government-related data;
- is considered a transaction that poses an unacceptable risk to national security;

- was initiated, is pending, or will be completed after the effective date of the executive order;
- does not qualify for an exemption (if any proposed under the called-for regulations; and
- is not ordinarily incident to and part of the provision of financial services or required for compliance with any federal statute, regulation, guidance or order.

The executive order also calls on the DOJ and relevant federal agencies to identify countries of concern and individuals (e.g., businesses) of concern, where such transfers of sensitive personal data may be prohibited or restricted. However, the executive order stops short of calling for regulations that outright prohibit all personal data transfer to such countries or businesses identified as "concerning."

The types of restrictions will also be-in theory-based on not only the sensitivity of the personal data and to what country it is being transferred to, but also on the **volume** of data being transferred.

While, on the surface, calling for strict regulations, the executive order also calls for a process through which business can seek licenses to authorize transactions that would otherwise be prohibited under the new, called-for regulations. So, there may end up being flexibility built into this new cross-border data transfer regime. Where such transactions are permitted, the executive order calls for the development of new required security measures and contractual requirements. The goal being to set forth security guidance that would mitigate potential risks posed by such high-risk transactions and transfers of sensitive personal data.

Conclusion

While federal omnibus data protection laws have puttered out and not advanced in a material way in the US, this new executive order marks a clear understanding by the federal government that regulating personal data and transfers thereof are critical. And expect the DOJ and relevant federal agencies to move fast.

In fact, the DOJ already announced an Advance Notice of Proposed Rulemaking. The DOJ also announced that the rulemaking will contemplate identifying China, Russia, Iran, North Korea, Cuba and Venezuela as "countries of concern" under the forthcoming regulations.

Businesses operating with offices, customers, and operations across the globe will need to maintain keen eyes on the rulemaking process as new regulations may govern what types of data they can transfer to non-US locations.

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

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.