Insights, News & Events

NEW EXECUTIVE ORDER TO BLOCK BUSINESSES FROM TRANSFERRING DATA TO CHINA AND OTHER COUNTRIES OF CONCERN – 4 STEPS TO COMPLY

Insights
Feb 29, 2024

President Biden just issued an Executive Order that will lead to new restrictions on transferring sensitive personal data to China and other "countries of concern" – and it may create massive new compliance obligations for your organization. While you might not think your business is in the data collection or transfer business, you may find yourself affected by yesterday's action because of tracking technology on your website or if any of your third-party vendors have access to personal data of employees or others. Here is what you need to know – and four steps you should take – to ensure your business is in compliance with this significant new requirement.

How We Got Here

The Executive Order is concerned about how foreign adversaries obtain Americans "bulk sensitive personal data" through legal means. The United States is still a Wild West when it comes to privacy laws. While some states have comprehensive laws, there is no federal or state comprehensive privacy law that prevents the transfer of data storage to foreign countries – or even that requires that foreign countries have laws in place to meet minimum standards of respecting data privacy.

This allows American data to flow to foreign countries with little hindrance. It can then be used to engage in malicious activities – such as espionage, intrusive surveillance, scams, blackmail, intimidation of political opponents, curbing dissent, limiting Americans' freedom of express and other civil liberty, and engaging in other violations of privacy.

Related People

Darcey M. Groden, CIPP/US

Partner

858.597.9627

Nan Sato, CIPP/E, CIPP/C

Partner

610.230.2148

These risks are compounded by the advent of more advanced artificial intelligence.

This Executive Order seeks to halt that unhindered data exodus by directing the Attorney General and the Department of Homeland Security to issue rules limiting what data can be transferred to "countries of concern." While this term is not defined in the Executive Order, it is widely understood that China is the main target.

This is for good reason. China's Personal Information Protection Law significantly limits outbound data transfers once the data are in China. In many situations, international transfers must be assessed by the Cyberspace Administration of China (CAC) first. This requirement gives the CAC almost unrestricted authority to access and review data it deems "important."

What Does the Executive Order Require?

The Executive Order itself defers the specifics to the AG and Department of Homeland Security, so this will be an evolving story. However, there are things that are clear now.

- First, the Executive Order defines sensitive personal data to include information about finances, genetic makeup, personal health, biometrics, geolocation, and other certain types of personally identifiable information – with a potentially broader definition to be created by the AG.
- Second, it will require the AG (with the assistance of Homeland Security) to issue regulations that will prevent the large-scale transfer of data to countries of concern, including determining what types of transaction pose an unacceptable risk to national security.
- Third, it will require the AG and Homeland Security to work together to set higher security standards to prevent access by countries of concern through other commercial means, such as data available via data brokerages, third-party vendor agreements, investment agreements, and employment agreements.

All Industries Are Affected

The reality is that no industry will escape the reach of this Executive Order – the better question is how or how much an industry will be affected.

Service Focus

Government Relations

International

Privacy and Cyber

At a general level, every business that operates a website needs to take a close look at what cookies, pixels, web beacons, and other tracking technologies they have on their website and whether they belong to a company located in a country on the "countries of concern" list.

- The obvious cornerstone of concern right now is TikTok, the popular social media platform owned by ByteDance Limited, a privately held company headquartered in Beijing, China.
- Pixels are pieces of code that can be used for by websites for things such as analytics and targeted advertising. Like cookies, they can track individuals across as they travel on different websites across the web, building a profile on the person based on their interactions with different websites.
- And, importantly for the Executive Order, all the information collected through the pixel is disclosed to TikTok.

Aside from your websites, you should look close at what companies and vendors you work with and whether information is being sent to countries of concern. While this review should not be limited to any particular industry, you may need to make serious adjustments to your practices if you are in the healthcare field. Of particular concern is genetic information given that many U.S. healthcare systems outsource genetic testing or genome sequencing to Chinese companies.

Your Next Steps

1. Review Your Website

Take a close look at your website to evaluate what cookies, pixels, web beacons, and other tracking tools are on it. Identify the company behind each tracking tool (including owners of that company) and what country it is located in so that you are prepared to act swiftly once the countries of concern are identified. Additionally, if you have any tracking tools which are owned by China (such as TikTok), you can act proactively to remove them now.

2. Conduct a Vendor Review

Conduct a review of vendors to whom you disclose sensitive personal information in order to evaluate whether any are

located in countries of concern. If they are, your business will need to find new vendors to fill that niche and stop doing business with any vendor located in a country of concern.

3. Seek Assurances

For your vendors to whom you disclose sensitive data who are not located in countries of concern, seek assurances that they will comply with the Executive Order and not transfer data to countries of concern. You may also consider negotiating contract terms to that effect moving forward.

4. Stay Alert

Stay tuned for further updates. The Executive Order calls for new regulations that will prohibit or restrict transactions that provide countries of concern access to either government-related data or sensitive personal data that poses an unacceptable national security risk.

Conclusion

The best way to stay alert is to make sure you are subscribed to Fisher Phillips' Insight System. We will provide the most up-to-date information on data security and the workplace directly to your inbox. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Privacy and Cyber Group.