LEXOLOGY

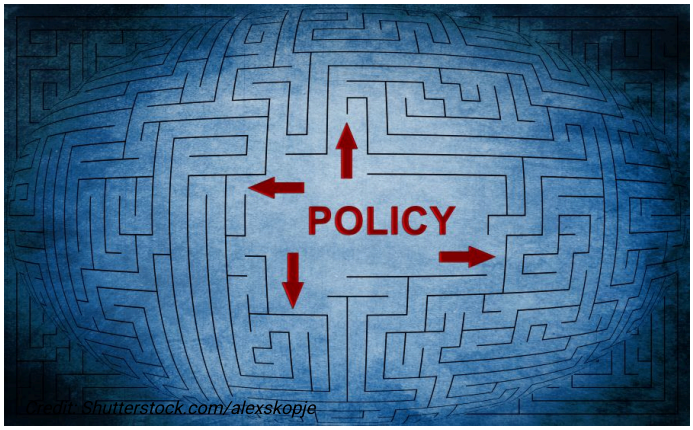
Seller beware: navigating third-party corporate ownership under new US data restrictions

Updated as of: **05 May 2025**

LEXOLOGY PRO

Saved | Forward | Share | Ask Lexy | Follow

Companies sharing US persons' bulk data need to account for third parties' ownership structures contractually and in due diligence to comply with new US data brokerage rules.



Credit: Shutterstock.com/alexskopje

The US Department of Justice (DOJ) issued guidance and a FAQs on 11 April 2025 regarding its new rule that restricts access to Americans' bulk sensitive personal data and US government-related data by China and other "countries of concern." Notably, the rule also applies to foreign entities that are 50% or more directly or indirectly owned by a country of concern, organised or chartered under that country's laws or that have their principal place of business in that country. Those entities are considered "covered persons," and are subject to inclusion on a non-exhaustive list of persons designated as such by the US attorney general.

The Biden-era rule took effect on 8 April 2025. However, the DOJ announced it wouldn't prioritise enforcement against any person for data security programme violations occurring between 8 April and 8 July 2025 if the person makes a good faith effort to comply with the programme during that time frame.

"Companies were waiting to see if there would be a shift with the new administration and enforcement priorities," said Morrison Foerster partner Kaylee Cox Bankston. "The answer, I think, is no."

Indeed, the Trump administration might pick up right where the Biden administration left off. During the IAPP's Global Privacy Summit keynote address in April 2025, US Federal Trade Commission (FTC) Commissioner Melissa Holyoak said the FTC may enforce the Protecting Americans' Data from Foreign Adversaries Act 2024 (PADFA).

That law prohibits data brokers from selling or disclosing US persons' biometrics, precise location data and other sensitive information to China, Russia and other foreign adversary countries and entities controlled by those governments. That legislation determines foreign adversary control similar to the DOJ rule, but with a lower ownership threshold (20%).

The DOJ's and FTC's new measures raise the stakes for companies to know what data they're sharing and with whom they're sharing it. However, lawyers told Lexology PRO that companies might be able to lean on the DOJ's recent guidance and other national security measures to assemble the due diligence needed to mitigate the new regulatory risks.

Ask questions, dig for answers

"Under both regimes, I think the practical guidance is similar," said Paul Weiss partner and former DOJ National Security Division assistant attorney general John Carlin. "You need to figure out, 'Hey if I'm doing business with a party, how much risk do I have in this transaction?'"

Carlin added that companies should also do "basic diligence," especially if they haven't previously worked with a particular business. For instance, companies can internally determine or use sanctions compliance vendors to determine what laws a business is subject to and its ownership structure.

Companies can also review a potential business partner's internal bylaws, ownership controls, parent companies and affiliates, added Morgan Lewis & Bockius partner and former US Federal Communications Commission (FCC) Enforcement Bureau chief Loyaan Egal.

"Even on its face, if it's not a company that is domiciled in a country of concern or a foreign adversary . . . it still requires you to do that level of due diligence," Egal said.

Contractual language

Wilson Sonsini partner Joshua Gruenspecht said companies can also add contractual clauses leveraged to comply with Committee on Foreign Investment in the United States reviews, government contracting and other federal measures.

"In all of those cases it's [about] your business counterparty doesn't necessarily want to tell you who their owners are [or] give you their capitalisation tables, if they are a privately owned company," Gruenspecht said. "The way we have fought that for years, in all of those spaces, and the way we will fall with PADFA and the DOJ is with representations in your legal contracts with other parties."

More companies will likely include attestations that the entity obtaining their bulk sensitive data isn't a country of concern or foreign adversary, but that isn't enough.

"A lot of companies are sending letters to companies saying, 'Please confirm you don't have individuals in these countries, you don't use vendors in these countries.' That's one way you can do it too," Morrison Foerster's Bankston said. She added, "Simply putting in a contract provision is not sufficient."

'Adequate due diligence'

Reliance on third-party attestations are a limited part of a larger due diligence process.

"I think DOJ has indicated, including in the preamble of the final rule, that companies should engage in a risk-based assessment, including screening vendors to see if they meet the definition of a covered person under this rule," said Covington & Burling special counsel Ingrid Price.

In addition to screening vendors against the DOJ's Covered Persons List, the regulator said companies should also determine if their vendors are listed on the Specially Designated Nationals and Blocked Persons list, the FCC's Covered List and other federal frameworks.

The DOJ's guidance also noted that US entities conducting "data brokerage" transactions with non-covered foreign persons and third countries can't "simply shift responsibility" to the other entity or rely upon contractual provisions.

"Depending on the circumstances, a U.S. person's failure to conduct adequate due diligence may subject the U.S. person to enforcement actions if that failure would constitute an evasion of the regulations, such as repeatedly knowing of violations by a foreign person and continuing to engage in data-brokerage transactions with that foreign person," the DOJ wrote.