Insights, News & Events

HOUSE REPUBLICANS UNVEIL NATIONAL DATA PRIVACY BILL: HERE'S WHAT EMPLOYERS AND BUSINESSES NEED TO KNOW

Insights
Apr 23, 2026

House Republicans Unveil National Data Privacy Bill: Here's What Employers and Businesses Need to Know

House Republicans just introduced sweeping federal data privacy legislation yesterday that could reshape how businesses collect, store, and use personal information, aiming to finally replace a growing patchwork of state laws with a single national standard. But the bill, known as the SECURE Data Act, faces significant hurdles before becoming law, so employers and businesses should approach it cautiously. This Insight will recap what you need to know about the bill and provide a few best practices all businesses can take when it comes to data privacy.

What Is the SECURE Data Act?

The Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act, introduced by Rep. John Joyce (R-Pa.) on April 22 and backed by House Energy and Commerce Committee Chair Brett Guthrie (R-Ky.), would create the first comprehensive federal consumer privacy framework in US history. The bill is the product of a Data Privacy Working Group that gathered input from more than 170 organizations and received over 250 written responses from stakeholders across industry, civil society, and government.

What Would It Require of Businesses?

Related People

Risa B. Boerner, CIPP/US, CIPM

Partner

610.230.2132

Benjamin M. Ebbink

Partner

The legislation builds on the framework already adopted by the majority of states that have enacted consumer privacy laws. It would impose several significant obligations on companies that process personal data above certain thresholds. Here are the key provisions employers and businesses need to understand.

Data Minimization

Companies would be required to limit their collection of personal data to what is "adequate, relevant, and reasonably necessary" for the purposes disclosed to consumers. Many state laws already include similar language, but a federal standard would make it universally applicable to businesses operating across state lines.

Consumer Rights

The bill would give consumers the right to access, correct, delete, and obtain a portable copy of their personal data. Consumers could also opt out of targeted advertising, the sale of their personal data, and certain automated profiling decisions. Sensitive data (including health information, financial data, precise geolocation, and more) could only be processed with a consumer's affirmative opt-in consent.

Teen Data Gets Special Treatment

One of the bill's more significant departures from the typical state framework: personal data about anyone under age 16 would be classified as sensitive data, requiring verified parental consent to process. This expands the age-13 threshold contained in the Children's Online Privacy Protection Act (COPPA) by three years and would have significant implications for any consumer-facing business that collects data from teenagers.

Data Broker Obligations

Data brokers would face new registration requirements with the Federal Trade Commission, which would maintain a public-facing registry. Brokers would also be subject to data minimization, disclosure, and security requirements under the bill.

Foreign Adversary Disclosures

Companies would be required to disclose when personal data is processed in or sold to China, Russia, or other

916.210.0400

Usama Kahf, CIPP/US

Partner

949.798.2118

Braden Lawes

Senior Government Affairs Analyst

202.916.7176

Service Focus

Consumer Privacy Team

Government Relations

Privacy and Cyber

designated foreign adversaries, a notable national-security addition not commonly seen in state privacy laws.

Two Big Wins for Businesses: Preemption and No Private Right of Action

The bill includes two provisions that businesses and employers have long sought in any federal privacy framework.

- First, the SECURE Data Act would strongly preempt state laws. Any state law or regulation that "relates to" the bill's provisions would be superseded by the federal standard. For multistate employers currently navigating a complex web of state privacy requirements – California, Colorado, Virginia, Texas, and nearly two dozen others – a single federal framework would represent a significant compliance simplification.
- Second, the bill does not include a private right of action. Enforcement would rest with the FTC and state attorneys general. This is a meaningful distinction from California's privacy regime, which has exposed companies to costly consumer lawsuits, and it aligns with how the majority of state privacy laws are structured.

The Road Ahead Is Daunting

Despite the bill's ambitions, passing it will not be easy. Republicans hold slim majorities in both chambers, and the Senate requires 60 votes to advance most legislation, meaning Democratic support will be essential. So far, no Democrats have signed on as key sticking points emerge:

- Several states, California chief among them, have resisted federal preemption of their stronger local standards. (And it's also worth noting that even some Republicans have expressed hesitation about preemption given their preference for strong state's rights, so universal GOP support for a measure that preempts state privacy laws is not guaranteed – which could make passage even more challenging given the razor-thin margins in both houses.)
- Democrats have historically pushed for a federal privacy law that sets a floor rather than a ceiling, allowing states to go further as technology evolves.
- Democrats have also consistently backed a private right of action, which the Republican bill deliberately omits.

- And while some Democrats have proven willing to support versions of this type of bill in the past, the political will to compromise may not be there if they believe they have a chance to take back Congress in November's midterm elections.

But it appears the GOP House strategy here is to have Energy and Commerce Committee Chair Guthrie and Financial Services Committee Chair Hill endorse the bill to grow support on the Republican side first, including those who were on the working group that Rep. Guthrie previously formed. They will then attempt to get as many Democrats on board as they can after they know they have the votes. Democrats might try to assert leverage and extract concessions from GOP leaders before agreeing to any sort of support.

The bill will next head to a subcommittee hearing, followed by markup sessions at both the subcommittee and full committee level. That process alone will take months, and negotiations between the parties are just beginning.

What Should Businesses Do Now?

Given the bill's uncertain path forward, sweeping compliance overhauls would be premature. But employers and businesses should still pay close attention, as the SECURE Data Act represents the most serious federal privacy push in years.

In the meantime, good data hygiene remains the right call regardless of what happens legislatively. Conducting an inventory of the personal data you collect, reviewing your data minimization practices, and ensuring you have appropriate consent mechanisms in place for sensitive data will position your organization well whether this bill advances or a future iteration ultimately crosses the finish line.

Conclusion

We will continue to monitor the SECURE Data Act as it moves through Congress and will provide more specific compliance guidance if and when it gains meaningful traction, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this

Insight, or any attorney on the firm's Privacy and Cyber Practice Group or Consumer Privacy Team.