DATA PRIVACY & GOVERNANCE HUB

SECURE Act Proposes Federal Data Privacy Framework

MAY 2, 2026

Key Takeaways

- House Republicans introduced the SECURE Act, which is the first comprehensive federal data privacy framework.
- This Act would preempt state laws and establish uniform national standards.
- The Act largely follows the models used by states but also includes heightened protections for minors and new national security requirements.
- Enforcement is handled by the FTC and state attorneys general, rather than through private civil suits, which simplifies compliance for businesses.

What Happened

House Republicans have recently introduced the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Act). This legislation, released on April 22nd, aims to establish “a national framework for consumer privacy rights and the protection of personal data.”

This is Congress’s first major attempt to establish comprehensive rules for consumer data privacy, aiming to replace the growing patchwork of compliance regulations enacted by individual states.

The Data Privacy Working Group, which produced the bill, gathered input from more than 170 organizations and received over 250 written responses from industry, civil society, and government stakeholders. Although it faces significant hurdles before being signed into law, this bill would reshape how businesses collect, store, and use personal information.

Privacy and Governance Concerns

The Act builds on the foundation set by many states in the U.S. and applies to a) entities that collect and process the personal data of more than 200,000 individuals annually and have a gross revenue of at least $25 million, or b) entities that collect and process data of at least 100,000 individuals and derive 25% or more of their annual gross revenue from selling that data.

The legislation includes distinct obligations for both data controllers and processors, heightened protections for sensitive personal data, opt-in consent (which also applies to teenagers), and a data broker registration list.

One of the more distinctive departures from the state framework seen across the country is that the personal data about anyone under the age of 16 would be classified as sensitive data and require parental consent to process, which is an extension of the current age cap at 13 years old set by COPPA (Children's Online Privacy Protection Act).

Additionally, companies would be required to disclose any instance in which data is sold to a designated foreign adversary, such as Russia or China, which is an important national security addition not common in state privacy laws.

Why It Matters / Policy Considerations

Notably, the SECURE Act would preempt any state laws that "relate to" the bill's provisions, superseding them by the new federal standard. This would significantly simplify compliance for businesses currently operating in a complex web of privacy requirements.

Additionally, enforcement would fall under the Federal Trade Commission and the state attorneys general. This is a distinct deviation specifically from California's privacy act, which has left companies vulnerable to costly consumer lawsuits.

The Act does not include any requirements for data protection impact assessments and defers universal opt-out standards to the Secretary of Commerce, which raises questions about the rigor of enforcement ability and potentially reduced consumer safeguards.

Overall, the SECURE Act marks meaningful progress towards federal privacy standards, though substantial legislative hurdles remain before enactment. The bill will next move to the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade for review.