DATA PRIVACY & GOVERNANCE HUB

Alabama Establishes Comprehensive Consumer Data Privacy Protections

APRIL 21, 2026

Key Takeaways

- The Alabama Personal Data Protection Act (APDPA) grants residents the right to access, correct, delete, and obtain copies of their personal data.
- Unlike many other state frameworks, the APDPA does not require data protection impact assessments or universal opt-out preference signals and includes broader exemptions than other state laws.
- Alabama joins a growing state-level patchwork of privacy laws, each with distinct thresholds and exemptions, underscoring the absence of a uniform federal framework.

What Happened

On April 16, 2026, the Alabama Personal Data Protection Act (APDPA) was signed into law, making Alabama the 21st state to establish comprehensive privacy protections. Although many other states followed the Virginia model of privacy legislation, Alabama's law deviates from this trend, particularly regarding the applicability thresholds, the definition of scale, and the potential for business exemptions.

This law comes amidst a growing number of data breaches and cyberattacks, as states continue to act in the absence of a federal privacy framework.

Privacy and Governance Concerns

Under APDPA, consumers' personal data is protected, meaning "any information that is linked or reasonably linkable to an identified or an individual who can be readily identified, directly or indirectly." This does not include de-identified data or publicly available information, like many

types of federally regulated data, employment and HR data, and data collected to comply with state law.

This law applies to (1) businesses that operate in Alabama or target Alabama residents and control the personal data of 25,000+ consumers, and (2) companies that derive 25% of revenue from selling personal data. However, the APDPA does not cover individuals acting in a commercial or employment context, which largely follows other state consumer privacy laws.

These thresholds make it easier for businesses to be covered than under the privacy laws of other states; however, they also include important exemptions that many other states don't have. Some entities that are not required to comply with the APDPA include two or four-year higher education institutions, HIPAA-covered businesses, and certain political action committees. As data security incidents become increasingly common, the exclusion of certain entities from compliance requirements raises questions about the consistency with which consumers are protected across sectors.

Why It Matters / Policy Considerations

Alabama's APDPA adds to the growing body of state-level privacy legislation, each with distinct thresholds, exemptions, and enforcement mechanisms due to a lack of federal privacy guidelines. The APDPA is unique in that it does not require data protection impact assessments or implement universal opt-out preferences. With more and more states across the country establishing their own frameworks, questions regarding consistency, accountability, and transparency are moving to the forefront for both consumers and businesses.