POLSINELLI

Publications

April 20, 2026 • Updates

Alabama Becomes Latest State to Enact Comprehensive Privacy Law

Alabama has joined the expanding patchwork of states enacting consumer privacy laws, with a new statute that will require many businesses to reassess how they collect, use and sell personal data. On April 16, 2026, Governor Kay Ivey signed into law the Alabama Personal Data Protection Act (APDPA), a comprehensive consumer data privacy law. The APDPA will take effect on May 1, 2027. The law applies to many companies doing business in Alabama or targeting its residents and introduces obligations around consumer rights, data use and transparency.

Key Takeaways:

- The APDPA largely follows the "Virginia model" of comprehensive consumer privacy laws, so many requirements will be familiar to companies with existing privacy programs.
- The APDPA's scope combines a low processing threshold with a broad small business exemption.
- The APDPA prescribes specific mechanisms for opting out of targeted advertising and the sale of personal data but does not include an express requirement for data protection assessments.
- If not already subject to other state privacy laws, companies in Alabama that fall in scope may face significant new compliance obligations.

Threshold and Exemptions

The APDPA differs from many other state privacy laws in that it combines a relatively low processing threshold with a broad small business exemption. The law applies to entities that conduct business in Alabama or target Alabama residents and either control or process the personal data of more than 25,000 consumers, excluding data processed solely to complete a payment transaction, or derive more than 25 percent of gross revenue from the sale of personal data.

Along with the exemptions we normally see, the APDPA also exempts businesses with fewer than 500 employees and nonprofits with fewer than 100 employees, provided they do not engage in the sale of personal data. In that respect, Alabama's scope may be

Related People

- Starr Turner Drum
- Ashleigh Bickford

Related Capabilities

- Privacy & Cybersecurity

narrower in reach than many other state consumer privacy laws, even though its consumer threshold is lower than the 100,000-consumer threshold used in several states and lower than the 35,000-consumer threshold used in states such as New Hampshire, Maryland and Rhode Island.

General Requirements

The APDPA generally follows the framework adopted by other state consumer privacy laws, like Virginia. Many organizations with existing compliance programs for other state privacy laws will find they are already aligned with the requirements of the APDPA. Key consumer privacy protections common to other state frameworks include:

- Standard consumer rights including access, correction, deletion and opt out of targeted advertising, sale and profiling
- Data processing agreements with specific safeguards between parties that are transferring personal data
- Opt-in consent for processing sensitive personal data
- Opt-in consent for processing personal data of minors between 13 and 16 for the purposes of targeted advertising or sale
- Data minimization and purpose limitation requirements
- Exemptions for data or entities subject to federal laws such as HIPAA, GLBA and FERPA

Opt-Out Mechanisms

The APDPA's approach to opt-out rights is consistent with other state privacy laws, requiring controllers to allow consumers to opt out of the sale of personal data and targeted advertising. However, the APDPA specifically requires that controllers provide on their website a clear and conspicuous link to a page that either (1) enables the consumer to directly opt out of processing for the purposes of targeted advertising or the sale of personal data or (2) provides up-to-date contact information for a consumer to submit an opt-out request. This requirement leaves little discretion for companies to decide how to go about opt-out requests — a clear and conspicuous website link directing consumers to a page where they can exercise their opt-out rights is required.

No Data Protection Assessment Requirement

Many state privacy frameworks require businesses to evaluate and document risks associated with activities such as targeted advertising, profiling or the processing of sensitive data, but the APDPA does not expressly require these assessments.

Enforcement

The Alabama Attorney General has sole enforcement authority. There is no private right of action. The Attorney General must provide companies with notice and a 45-day opportunity to cure before bringing an action. If the violation is not cured, a court may assess a civil penalty of up to $15,000 per violation.

What Should Companies Do to Prepare?

Alabama businesses not already in scope of other state privacy laws should evaluate whether they fall within the APDPA's applicability thresholds. For businesses that are in scope and have not yet implemented a privacy compliance program, the law will impose significant new obligations, including establishing processes to respond to consumer rights requests, developing and maintaining a compliant privacy notice, reviewing and updating vendor contracts related to the processing of personal data, and ensuring that

websites and other consumer-facing data collection tools (e.g., mobile apps) include a clear and conspicuous mechanism for consumers to exercise their consumer rights.

For questions about how to get started with privacy compliance, please contact Polsinelli's Privacy team.