



Alabama Personal Data Protection Act ("APDPA") Compliance Snapshot

Understand the Law. Identify Your Obligations. Prepare for Compliance.

This CLIClaw Compliance Snapshot provides a concise overview of the Alabama Personal Data Protection Act ("APDPA"), including its applicability, consumer privacy rights, key business obligations, third-party requirements, enforcement provisions, and compliance considerations.

Designed as a practical reference for businesses, the snapshot helps organizations understand the law's principal requirements, evaluate potential applicability, and identify areas that may require additional compliance planning or operational review.

Use this snapshot as a starting point for understanding Alabama's privacy requirements and determining whether further assessment, implementation, or legal guidance is needed.

DISCLAIMER

These materials are provided for informational and compliance support purposes only and are not intended as legal advice. Use of these materials does not establish an attorney-client relationship.

Organizations are responsible for evaluating applicable legal requirements and should consult qualified legal counsel regarding specific obligations.

CLIClaw makes no warranties regarding the completeness or applicability of these materials and disclaims liability for reliance on their use.

ALABAMA PERSONAL DATA PROTECTION ACT (APDPA) COMPLIANCE SNAPSHOT

Act 2026-552 (HB 351) | Enacted April 17, 2026 | Effective May 1, 2027



Alabama's privacy law establishes consumer rights and responsibilities for covered organizations handling personal data.

01

APPLICABILITY

Which Organizations May Be Covered?



- Doing business in Alabama or targeting Alabama residents, and either processing personal data of more than 25,000 consumers (including payment-only data), OR deriving more than 25% of gross revenue from personal data sales regardless of consumer count. Statutory exemptions apply.

02

CONSUMER RIGHTS

What Rights Do Alabama Consumers Have?



- Confirm and access their personal data.
- Correct inaccuracies.
- Request deletion.
- Obtain a portable copy of their personal data.
- Opt out of targeted advertising and personal data sales.

03

KEY BUSINESS OBLIGATIONS

What Must Covered Organizations Do?



- Provide clear and accessible privacy notices.
- Establish consumer-request processes.
- Implement data minimization.
- Obtain consent for sensitive data.
- Comply with consumer opt-out requirements.
- Maintain reasonable security safeguards.
- Provide clear website opt-out methods for targeted advertising and data sales.

04

THIRD-PARTY REQUIREMENTS

What Applies to Processors and Data Sharing?



- Use written contracts with processors that meet statutory requirements.
- Ensure appropriate oversight of processor activities.
- Evaluate third-party sharing arrangements, including personal data sales and targeted advertising.

05

COMPLIANCE READINESS

What Should Organizations Do Now?



- Assess whether the law applies to your organization.
- Review and update data practices.
- Update privacy notices and opt-out methods.
- Evaluate vendor and third-party arrangements.

06

ENFORCEMENT

How Is the Law Enforced?



- Enforced by the Alabama Attorney General.
- The Attorney General must provide notice of an alleged violation and a statutory opportunity to cure.
- Violations may result in civil penalties of up to \$15,000 per violation.



Opt-out signals: The enacted law does not impose a broad universal signal-recognition mandate; specific statutory signal-related provisions still apply.



Need to Put Alabama's Privacy Requirements Into Practice?

Explore CLIClaw's Privacy Compliance Solutions for assessments, procedures, checklists, and documentation tools.

[Explore Privacy Compliance Solutions →](#)



CLIClaw
Center for Legal Internet Compliance

General information only, not legal advice.
Practical Solutions. Greater Compliance.

CLIClaw.com | © 2026 CLIClaw LLC

