



ALABAMA PERSONAL DATA PROTECTION ACT (APDPA)

CHECKLIST



 **USERCENTRICS**

Alabama Personal Data Protection Act (APDPA) gives Alabama residents rights over how their personal data is collected and used.

This checklist walks through steps that support your compliance efforts under the Act, along with recommended best practices for privacy-related user experience.



Important to know:

Action	Date
Effective date	May 1, 2027
Retroactive	No

1 Determine If Your Company Is Required to Comply

If your organization conducts business in Alabama or targets Alabama residents, and either:

- Controls or processes the personal data of more than 25,000 consumers annually (excluding data processed solely to complete a payment transaction), or
- Derives more than 25 percent of gross revenue from the sale of personal data, regardless of consumer volume

There is no minimum annual revenue floor, and this low consumer threshold brings a wider range of businesses into scope.

Exemptions include:

- Political subdivisions
- Higher education institutions
- [GLBA](#)-regulated financial institutions
- [HIPAA](#)-covered entities
- Businesses with fewer than 500 employees that do not sell personal data
- Nonprofits with fewer than 100 employees that do not sell personal data

2 Create a Comprehensive Privacy Policy

Businesses are required to disclose:

- Categories of personal data processed
- Purposes for processing
- Categories of personal data and third parties shared with, if any
- An active email address or other contact mechanism
- How consumers may exercise their rights, including a link to the required opt-out method

If your business sells personal data or processes it for targeted advertising, disclose this clearly and conspicuously in your [privacy policy](#), along with the opt-out method. For example, use a [Privacy Policy Generator](#) and a [CMP to manage opt-outs](#).

3 Inform Consumers About Their Rights

Consumers' rights under the APDPA:

- **Right to access:** Confirm processing and access personal data (subject to trade secret protection)
- **Right to correct:** Fix inaccuracies in personal data
- **Right to delete:** Request deletion, with some exceptions
- **Right to portability:** Obtain a portable copy where processing is automated
- **Right to opt out:** Of targeted advertising, sale of personal data, and profiling used in solely automated significant decisions
- **Right to non-discrimination:** For exercising these rights

A parent, guardian, or conservator may exercise rights on behalf of a known child under 13 or another consumer, as applicable.

4 Provide a Clear and Conspicuous Opt-Out Method

Provide a link on your website enabling consumers to opt out of targeted advertising and the sale of personal data directly, or up-to-date contact information for submitting an opt-out request. Where an opt-out preference signal conflicts with an existing privacy setting or loyalty program, honor the signal but you may notify the consumer of the conflict.

5 Authenticate Consent for Collection of Sensitive Personal Data or Data From Minors

Sensitive personal data: Obtain the consumer's affirmative, opt-in consent before processing [sensitive personal data](#). Unlike California's opt-out model, the APDPA requires consent upfront, not an opt-out mechanism after the fact.

Minors aged 13–15: Obtain opt-in consent from the consumer before processing their personal data for targeted advertising or sale of personal data, when a controller has actual knowledge the consumer falls in this age range.

Known children (12 and younger): Obtain consent from a parent or legal guardian, consistent with COPPA, before processing personal data concerning a known child.

6 Handle Children's Data in Line With COPPA

Personal data from a known child under 13 is classified as sensitive data. Controllers that meet [COPPA](#)'s verifiable parental consent requirements are deemed compliant with the APDPA's parental consent obligation.

7 Provide a Consent Revocation Mechanism

Revocation must be at least as easy as the method used to give consent. Once a consumer revokes consent, stop the relevant processing as soon as practicable, and no later than 45 days after the request.

8 Audit Consent Interfaces for Dark Patterns

Consent obtained through a [dark pattern](#) is invalid under the APDPA. This includes any interface designed to subvert or impair a consumer's autonomy or choice.

9 Review Data-Sharing Arrangements Against the APDPA's "Sale" Definition

Alabama's definition of "sale" is broader than several comparable state laws. It covers exchanges for monetary or other valuable consideration, where the controller receives a material benefit and the recipient's use of the data is unrestricted. Arrangements exempt elsewhere may qualify as a sale here.

10 Enable and Respond to Data Subject Access Requests (DSARs)

Respond to [DSARs](#) within 45 days, extendable by a further 45 days with notice to the consumer. Provide responses free of charge once per 12-month period per consumer. Manifestly unfounded, excessive, or repetitive requests may be charged a fee or declined. The burden of demonstrating this falls on the business.

11 Establish an Appeal Process

If a request is denied, provide an appeal process. If the appeal is denied, direct the consumer to the Alabama Attorney General.

12 Maintain Written Processor Contracts and Conduct Data Protection Assessments

Govern processor relationships with a written agreement covering instructions, data types, duration, and obligations. Conduct [data protection impact assessments \(DPIAs\)](#) for high-risk processing beginning on or after May 1, 2027. High-risk processing includes targeted advertising, data sales, profiling, and sensitive data processing.

**Falling thresholds, rising enforcement and litigation,
eroding ad revenue. Do you know your risk?**

GET IN TOUCH