Insights, News & Events

ALABAMA ENACTS SWEEPING CONSUMER PRIVACY LAW: 7 STEPS YOUR BUSINESS SHOULD CONSIDER TO PREPARE

Insights
Apr 17, 2026

Alabama Enacts Sweeping Consumer Privacy Law: 7 Steps Your Business Should Consider to Prepare

Alabama just joined 20 others states by enacting a comprehensive consumer privacy law, and businesses must get ready to comply with sweeping new obligations that will kick in next year. The state's new Alabama Personal Data Protection Act (APDPA), signed into effect yesterday by Governor Ivey, establishes a broad privacy framework for how businesses collect and sell consumers' personal data. We'll explain key aspects of the new law and offer seven steps you can take now to prepare.

Table of Contents

Related People

Ree Harper
Partner

205.963.5403

Raymond W. Perez
Of Counsel

205.963.5400

Overview

Governor Kay Ivey just signed a bill (HB 351) into law that establishes the Alabama Personal Data Protection Act (APDPA). The new law, which takes effect **May 1, 2027**, establishes:

- data privacy rights for consumers;
- duties for "controllers" (see "Controllers vs. Processors" below);
- duties for "processors" (see "Controllers vs. Processors" below); and
- enforcement measures.

While the law imposes extensive obligations on covered businesses, it also includes many broad exemptions and carve-outs. We'll cover some of the highlights below, but you should work with counsel to understand whether and how the APDPA applies to your business in various specific data processing situations.

Scope and Applicability

Covered Consumers

The APDPA aims to protect consumers who are residents of Alabama. Importantly, however, it does not cover individuals acting in a commercial or employment context or as an employee, owner, director, officer, or contractor.

The APDPA's employment-data exception is consistent with all other state consumer privacy laws, except for the California Consumer Privacy Act (CCPA), which broadly defines "consumer" to include job applicants, current and former employees, and more.

Covered Data

Service Focus

Consumer Privacy Team

Data Protection and Cybersecurity

Privacy and Cyber

Related Offices

Birmingham

The APDPA protects consumers' personal data, which means any information that is linked or reasonably linkable to an identified or an individual who can be readily identified, directly or indirectly.

However, "personal data" does **not** include deidentified data (so long as the controller possessing the data complies with certain conditions) or publicly available information. In addition, the new state law specifies various types of data that are **not** covered by the APDPA, including, for example:

- **many types of federally regulated data**, such as protected health information under HIPAA or consumer reporting data covered by the Fair Credit Reporting Act;
- **employment and HR data**, such as information related to job applicants, current employees, contractors, or agents, as well as certain emergency contact and benefits administration data; and
- **data or information collected or processed to comply with state law.**

Covered Businesses

The APDPA applies to businesses that:

- operate in Alabama **or** produce products or services that target residents of the state; **and**
- control or process the personal data of more than 25,000 consumers **or** derive more than 25% of gross revenue from the "sale of personal data" (see below for more details).

Sale of Personal Data. Under the APDPA, a sale of personal data occurs (subject to any applicable exclusions) when a controller sells a consumer's personal data to a third party (without restricting how the third party may use that data in the future) in exchange for monetary or "other valuable" consideration that materially benefits the controller. While some states define the sale of data strictly to mean disclosures in exchange for monetary consideration, Alabama joins the batch of states that expand the definition to include disclosures in exchange for other things of real value, not just monetary consideration. But unlike other states, Alabama limits this "other valuable" category to only

consideration that materially benefits the controller. In the context of website cookies, this definition may implicate the sharing of data through certain cookies unless the following exception applies. The APDPA includes some **significant carveouts** from what would be considered selling of data (in addition to other standard types of exclusions included in most state consumer privacy laws) for certain types of data disclosures or transfers. For example, under the Alabama law, the disclosure or transfer of personal data to a third party for the purposes of providing **analytics services** or providing **marketing services** solely to the controller will not be treated as sales of personal data.

Notably, these thresholds make it easier for a business to be covered compared to the thresholds under other states' privacy laws. However, the new law provides various important exemptions, many of which go far beyond the exemptions available under other state laws of this kind. For example, the following entities will **not** be required to comply with the APDPA:

- Political subdivisions of the state, or any board, authority, district, or public corporation.
- Two-year or four-year institutions of higher education, as well as their affiliates.
- National registered securities associations.
- Certain federally regulated financial institutions and their affiliates.
- HIPAA covered entities or business associates.
- Businesses with fewer than 500 employees, so long as the business does not engage in the sale of personal data.
- Nonprofit entities with fewer than 100 employees, so long as the entity does not engage in the sale of personal data.
- Certain regulated industries.
- Trade associations explicitly authorized to receive certain documents or evidence from state insurance regulators.
- Certain political action committees, political parties, or principal campaign committees, and political

organizations, as well as businesses that primarily sell data to them.

- Electric providers subject to national reliability standards.

Controllers vs. Processors

If a business is covered by the APDPA, it must meet certain compliance requirements, which vary depending on whether the business is a "controller" or a "processor." Here's what these terms mean:

- A **controller** is an "individual or legal entity that, alone or jointly with others, determines the purposes and means of processing personal data."
- A **processor** is an "individual or legal entity that processes personal data on behalf of a controller."

Whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends on criteria laid out under the APDPA.

Controller Duties

Complying With Consumer Requests

A controller must comply with a consumer's authenticated request to invoke any of their rights under the APDPA, including requests for the controller to:

- Confirm whether the controller (or a processor or third party acting on its behalf) is processing the consumer's personal data and accessing any of their personal data under its control – unless confirmation or access would require the controller to reveal a trade secret.
- Correct inaccuracies in the consumer's personal data, considering the nature of it and the purposes for processing it.
- Delete the consumer's personal data.
- Provide a copy of the consumer's personal data (as previously provided by the consumer to the controller) in a format that meets certain conditions – unless providing the data would require the controller to reveal a trade secret.

- Allow the consumer to opt out of the processing of their personal data for the purpose of targeted advertising, sale of the data, or profiling in connection with solely automated significant decisions concerning them.

If a consumer is a child under age 13, these consumer rights may be exercised by their parent or legal guardian (and the same is true for guardian-consumer or conservator-consumer relationships, regardless of age).

In addition, controllers will be required to establish a secure and reliable method for consumers to exercise these rights and to follow certain procedures when handling consumers' requests, including, for example:

- responding to the consumer within 45 days after receiving their request (extensions are available under specific conditions) and, if applicable, provide justification for declining the request; and

- providing information in response to an authenticated request **free of charge** once per consumer during any 12-month period (subject to limited exceptions that allow the controller to charge the consumer a reasonable fee).

Other Controller Duties: Data Minimization, Consumer Privacy Notice, and More

The APDPA will impose many other compliance requirements on controllers. As just a few examples, controllers will be:

- limited to collecting personal data that is "adequate, relevant, and necessary" in relation to the purpose for processing it;

- required to establish and maintain "reasonably administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue";

- prohibited from, among other things, processing personal data for purposes that are not compatible with the disclosed purposes for processing it or processing a consumer's "sensitive data" without obtaining their consent (note: personal data of a known child under age 13 must be processed in accordance with the federal Children's Online Privacy Protection Act);

- required to provide consumers with a privacy notice that meets certain criteria; and
- required to handle deidentified data in accordance with specific rules.

Notably, however, the APDPA stops short of imposing several significant requirements that are included in consumer privacy laws in many other states. For example, the APDPA does **not** require controllers to conduct data protection impact assessments or implement universal opt-out preference signals.

Processor Duties

Processors will be required to adhere to the controller's instructions and take measures to assist the controller in complying with its obligations under the APDPA. The law also establishes requirements for contracts between controllers and processors.

Enforcement

Alabama's attorney general will have the power to enforce the APDPA and will be required to issue a notice of violation to the controller before initiating any action against it. The controller will then have 45 days to correct the alleged violation and notify the attorney general of the correction – if it fails to do so, the AG may bring an action in court, and, if the court finds against the controller, it may assess a civil penalty of up to **$15,000 per violation**.

7 Steps Your Business Should Consider Taking Now

If your business is covered by the APDPA, here are six steps you should consider taking now ahead of the law's May 1, 2027, effective date:

- **Evaluate** your organization's current data collection and privacy procedures.
- **Review existing privacy notices and policies**, including those drafted for compliance with the laws of other jurisdictions that have passed similar consumer privacy legislation.
- **Implement systems** to respond to authenticated consumer requests to invoke their rights under the APDPA.

- **Consider engaging in a data mapping exercise**, if your business has not done so recently, to identify consumer data your organization has collected and where that data resides.
- **Identify third parties** with whom your business shares consumer data and any existing data processing agreements with those entities.
- Assess your collection of data concerning **minors** (if any).
- **Stay tuned for updates** and work with data privacy counsel to evaluate your business's readiness for compliance with the APDPA.

Conclusion

As consumers demand more transparency about who receives their data and what it's used for, and without progress on a federal data privacy scheme, we expect more proposed legislation at the state level, as 20 other states have already enacted similar laws – including, most recently, the Oklahoma Consumer Data Privacy Act enacted last month.

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You can also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, any member of our Privacy and Cyber team or any attorney in our Birmingham office.