

Vital Briefing | Cybersecurity Policy Report

Alabama's Comprehensive Privacy Law: You May Be Surprised

By [Tony Foley](#), Senior Legal Analyst

Key Takeaways

- Alabama's new privacy law takes effect on May 1, 2027
- The law's applicability thresholds are surprisingly inclusive, but somewhat offset by a wide expanse of exemptions and other business-friendly provisions
- Data protection impact assessments are not required under the law

Overview. On April 16, 2026 Governor Kay Ivey (R.) signed [H.B. 351](#), Reg Sess. (Ala. 2026), making Alabama the 22nd state to enact a comprehensive privacy and data protection law, coming on the heels of Oklahoma's privacy law, which was enacted in March (see our [Vital Briefing](#) for a breakdown of the Oklahoma law).

The new law takes effect on May 1, 2027. It is described by most observers as a "business-friendly" regime, using a structure similar to the Virginia Consumer Data Privacy Act, but it's important to note that Alabama has enacted a few unexpected wrinkles in the law. The chart on page 2 provides a high-level summary of the provisions of the Alabama law.

What to know. Negotiations leading to the final version of the law as enacted yielded a number of surprising provisions. Chief among these is the law's expansive applicability provisions. Unlike most states, which include revenue thresholds tied to the number of consumers from which businesses collect personal data, [H.B. 351](#)

applies to persons that conduct business in Alabama or produce products or services targeted to state residents and that meet either of the following requirements:

- Control or process the data of more than 25,000 consumers (excluding personal data controlled or processed solely for the purpose of completing a payment transaction); or
- Derive more than 25% of gross revenue from the sale of personal data, **regardless of the number of consumers whose data the person controls or processes** (emphasis added).

The 25,000-consumer threshold for collection and processing is the lowest in the nation (excepting Texas, which does not have either a revenue or consumer volume threshold but exempts "small businesses" as defined under federal law). In addition, Alabama's revenue from sales threshold is unique among state privacy laws; every other state (again, excepting Texas) contains a minimum number of consumers from whom data is collected before applying the revenue percentage threshold. As a result, at first glance, Alabama's law seems to pull in more businesses than the vast majority of states with similar laws.

However, [H.B. 351](#) contains other provisions that are designed to narrow its applicability, including an entity-level exemption for businesses with fewer than 500 employees and nonprofits with fewer than 1,000 employees, provided that such businesses do not sell personal data. Other exemptions in the law apply to political subdivisions,

specified higher education institutions, financial institutions governed by the Gramm Leach Bliley Act (GLBA), HIPAA-covered entities and business associates, and political action committees, political parties and political campaign committees. The law also exempts specified types of data, including employee and business-to-business data, protected health information under HIPAA, and data governed by a number of federal laws including the FCRA, FERPA, DPPA, and Farm Credit Act.

From a political perspective, the juxtaposition of the surprisingly expansive applicability thresholds against the broad exemptions provided, particularly for small businesses, could indicate that legislators were anxious to blunt potential criticism that the law is too narrow while simultaneously limiting the compliance burden on businesses.

Other notable provisions of the law include the following:

- A carve-out of the disclosure or transfer of personal data to a third party for purposes of providing analytics services or for providing marketing services solely to the controller from the definition of a "sale" subject to the law's requirements;
- Adoption of relatively typical children's privacy provisions, including a definition of a "known child" as including children under age 13, in line with the federal Children's Online Privacy Protection Act (COPPA), and providing that controllers complying with COPPA's requirements regarding verifiable parental consent are

Applicability	Persons that do business in or target the state and a. Control or process data of 25,000 consumers (except for purposes of completing a payment transaction); or b. Derive more than 25% of gross revenue from sales of data, regardless of the number of consumers whose data the person controls or processes
Consumer Rights	• Access and verify the processing of their data • Correction • Deletion • Data portability • Opt-out rights for targeted advertising, sale or profiling in furtherance of decisions producing legal or similarly significant effects
Controller Obligations	• Provision of privacy policy to consumers • Data minimization • Data security requirements • Limitations on collection and processing of sensitive data
Exemptions	• Businesses with fewer than 500 employees that do not sell personal data • Nonprofits with fewer than 1,000 employees that do not sell personal data • State agencies and political subdivisions • Entities and data covered by HIPAA • Entities covered by GLBA • Higher education institutions • Specified political organizations • Employee and B2B data • Data regulated by other federal laws
Enforcement	• Exclusive enforcement by Attorney General • 45-day cure period, NO sunset • Civil penalties up to \$15,000/violation • NO private right of action

deemed with the law's consent requirements; and

- A non-sunsetting 45-day cure period for alleged violations.

Items that many other states have addressed recently that did not make their way into the enacted version of [H.B. 351](#) include the following:

- No requirement to conduct data protection impact assessments (DPIAs);
- No requirement to recognize universal opt-out preference signals (included in

various versions of the bill but removed by the Senate in the lead-up to enactment); and

- No private right of action (although, unlike other states, the law does not expressly prohibit such actions, it simply does not address the issue).

What to do. Businesses subject to the provisions of [H.B. 351](#) have some time to prepare, but the law's specifics should be analyzed right away to address several somewhat unique compliance challenges. Specifically, a business should carefully

review data sharing practices applicable to third parties to determine if they may be subject to the carve-out from the definition of a "sale" for analytics services and for providing marketing services solely to the controller. In addition, while the exemptions for small businesses and nonprofits would seem to be very enticing, it is critical for such businesses to verify that they do not engage in any sale of personal data. All told, however, businesses should face lighter compliance burdens than those required in more consumer-friendly states.

More to come? Maine very nearly beat Alabama in becoming the latest state with a comprehensive law, but [L.D. 1922](#), Reg Sess., failed to gain final approval in the legislature, with the state House voting down the Senate's final proposal on April 19, 2026, primarily based on strong lobbying efforts from businesses who objected to the bill's restrictive data minimization requirements ([Cybersecurity Policy Report, Apr. 10](#)).

That said, several states are on the cusp of enacting comprehensive legislation, including:

- Pennsylvania [H.B. 78](#), Reg Sess., passed by the state House last October and pending

in a Senate committee, which would establish a privacy regime with relatively low applicability thresholds and stringent restrictions on processing of sensitive data that could have a significant impact on businesses.

- Louisiana [H.B. 386](#), Reg Sess., approved by the state Senate on Apr. 8 and pending in the House Commerce Committee, which would confer consumer rights and impose controller obligations similar to those in Virginia; and
- Vermont [S.B. 71](#), Reg Sess., passed by the state Senate last year and pending in the Commerce and Economic Development Committee, which would enact consumer rights and controller obligation

provisions that generally are considered consumer-friendly, including stringent registration and data deletion requirements applicable to data brokers.

In addition, while not a new law, Connecticut [S.B. 4](#), Reg Sess., approved by the state House on May 4 after Senate approval in April, would amend the Connecticut Data Privacy Act (CTDPA) to, among other things, establish data broker registration requirements and establish additional restrictions on the processing of sensitive personal data.

For further information on these and other state privacy proposals, consult the [State Privacy and Cybersecurity Legislation Tracker](#) on Wolters Kluwer's VitalLaw Cybersecurity & Privacy dashboard.