Jul 01, 2025

Categories:

Publications

Technology Blog

Authors:

Mason C. Clutter

Caleb S. Long

Privacy Legislation | July 2025 Update

This month, two of the 19 comprehensive state-level consumer privacy laws come into effect: Tennessee's and Minnesota's. While both laws, in large part, bare a strong resemblance to the laws of many states that have come before them, each offers its own unique contribution to the patchwork of U.S. privacy laws.

Here are some key aspects of the Tennessee law to help you assess whether your business may be subject to the law and, if so, what it requires. Stay tuned for our next update on the Minnesota law later this month.

Tennessee Information Protection Act

Effective Date

July 1, 2025

Who is Impacted?

- Businesses that do business in Tennessee or direct products towards residents of Tennessee, who exceed $25,000,000 in revenue, and either—
    - Control or process the personal information of at least 175,000 consumers in a calendar year; or
    - Control or process the personal information of at least 25,000 consumers in one calendar year and derive 50% or more of their gross income from the "sale" of personal information.
        - "Personal information" is defined as information that is linked or reasonably linkable to an identified or identifiable natural person. This does not include information that is publicly available information or de-identified or aggregated consumer information.
        - "Controller" is defined as the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal information.
        - "Processor" is defined as a natural or legal entity that processes personal information on behalf of a controller. "Process" includes all actions taken on personal information,

such as collection, use, sharing, selling, and deleting.

- "Consumer" is defined as a natural person who is a resident of Tennessee acting only in a personal context and, therefore, does not include a natural person acting in a commercial or employment context.
- "Sale" is defined differently in the Tennessee law compared to other state consumer privacy laws. It is defined in this law as "the exchange of information for valuable monetary consideration by the controller to a third party," excluding from its definition "other valuable consideration" governed by other state consumer privacy laws.

A Few Key Exemptions

The Tennessee Information Protection Act provides for the following exemptions:

- Non-profit organizations
- Institutions of higher education
- Information governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act, and the Family Education Rights and Privacy Act
- Use of personal information for specific purposes, such as compliance with applicable laws, preventing fraud or injury, and defending legal claims

What To Know if You Are Covered by the Act

- **Consumer rights**: Tennessee Consumers have the following rights:
  - Confirm whether a covered entity is processing the consumer's personal information;
  - Access the consumer's personal information;
  - Correct personal information the consumer previous provided to a covered business;
  - Delete personal information (information from or about the consumer) that is not maintained in aggregated or de-identified form;

- Obtain a copy of the personal information the consumer previously provided to a covered business (i.e., the right to "data portability");
- Opt out of the sale of the consumer's personal information, use for targeted advertising, or "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer";
- Appeal a denial of a consumer's rights request; and
- Be free from discrimination for exercising a consumer right.

- **Data minimization standard**: Covered entities must limit their collection of personal information to what is "adequate, relevant, and reasonably necessary" for the purposes for which they process the personal information, as disclosed to consumers. Additionally, covered entities may only process personal information for purposes that are "reasonably necessary and compatible" with the disclosed purposes for processing unless they first obtain the consumer's consent.
- **Data security**: Covered businesses must maintain "reasonable administrative, technical, and physical data security practices" proportionate to the volume and nature of the personal information they collect.
- **Sensitive personal information**: Covered businesses must obtain consent from the data subject (or, in the case of a known child under the age of 13, in accordance with the Children's Online Privacy Protection Act) before collecting and processing "sensitive personal information."
    - "Sensitive personal information" includes personal information that reveals an individual's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; biometric information (if collected and/or used for the purpose of uniquely identifying an individual); personal information collected from a known child; and precise geolocation data.

- **Privacy policy**: Covered businesses must provide a privacy notice that includes specified elements, including the categories of personal information collected, how and why that information is collected and used, with whom it is shared, and how an individual may exercise their consumer rights.

- **Contracts with processors**: Covered entities must enter into a written contract with data processors (e.g., service providers, contractors, or other third parties with whom they share data), including any data-handling measures required to safeguard privacy and other elements required by the law.
- **Data protection assessments**: Covered entities must complete data protection assessments for specified activities, including the use of personal information for targeted advertising, the sale of personal information, the processing of personal information for purposes of profiling, the processing of sensitive personal information, and processing activities that "present a heightened risk of harm to consumers."
    - Data protection assessments identify (a) the potential risk and benefits of the proposed processing activities to the consumer, other stakeholders, and the public; and (b) any appropriate mitigation measures employed by the business to mitigate the identified potential risks.

Enforcement

- **No private right of action**: The Tennessee Attorney General and Reporter has exclusive authority to enforce this regulation. There is no private right of action for consumers to bring suit under the law.
- **Cure period**: Before initiating an action, the Attorney General and Reporter must provide a covered entity with written notice of the provisions of the regulation allegedly violated and give the covered entity 60 days to cure the noticed violation.
- **Penalties**: If a covered entity fails to cure a suspected violation, the Attorney General and Reporter may initiate an action, seeking any of the following:
    - Declaratory judgment that the act or practice violated the law;
    - Injunctive relief, including preliminary and permanent injunctions, to prevent an additional violation of and compel compliance with the law;
    - Civil penalties of up to seven thousand five hundred dollars ($7,500) for each violation and up to treble damages if a court finds that the covered entity "willfully or knowingly" violated the law;

    - Reasonable attorney's fees and investigative costs; or
    - Other relief that the court deems appropriate.

- **Affirmative defense**: Tennessee's consumer privacy law is unique because it provides a covered entity with an affirmative defense to an alleged violation of the law. In short, an entity may demonstrate its reasonable conformance to the National Institute of Standards and Technology (NIST) Privacy Framework or certain certification options, such as those under the Asia Pacific Economic Cooperation's Cross Border Privacy Rules system, and provision of consumer privacy rights consistent with the law.

What to Do Now?

This is just a snapshot of some of the key features of the Tennessee Information Protection Act. If you think you may be covered by this or other U.S. state privacy laws, please contact your attorney to ensure your data privacy and security practices appropriately comply with the law. While compliance can be challenging, there are many ways in which a business can comply that account for their practices and the ways in which they engage with their consumers.

At Frost Brown Todd, we view compliance as an opportunity to not only comply with the law but to build and maintain trust with your customers while saving time and resources along the way. If you have questions or need immediate assistance, please contact the authors or any attorney with Frost Brown Todd's Data Security and Privacy team.

And keep an eye out for updates on other upcoming data privacy laws, such as the Kentucky Consumer Data Protection Act, the Indiana Consumer Data Protection Act, and the Rhode Island Data Privacy Act, all effective January 1, 2026.