



# TENNESSEE

## Information Protection Act

---

PROVIDED BY BAKER DONELSON  
Last updated: January 2025

*Please note this is a highlighted overview and not a complete overview of privacy laws for this state. If you would like a complete review of this state's privacy laws or a multi-state privacy compliance cheat sheet on specific topics, please contact Vivien Peaden at [vpeaden@bakerdonelson.com](mailto:vpeaden@bakerdonelson.com).*

*Disclaimer: These materials do not constitute legal advice and should not be substituted for the advice of legal counsel.*

# The Tennessee Information Protection Act (TIPA)

Effective Date: July 1, 2025

1. **Applicability Thresholds:** Subject to certain entity-level and data-level exemptions, the TIPA applies to a natural or legal person conducting business in the State of Tennessee or producing products or services targeted to Tennessee residents (**consumer**):



having **\$25 million or more in revenue**; and

controlling or processing:



**175,000+** Tennessee consumers' personal information;

or



**25,000+** Tennessee consumers' personal information and derive more than **50 percent of its revenue** from the sale of personal information.

2. **Key Definitions:**



**Sales of Personal Information:** "Sale of personal information" is narrowly defined as the exchange of personal information for **valuable monetary** compensation subject to certain exemptions.

3. **Business Obligations:** The TIPA imposes additional obligations on persons who, alone or jointly with others, determine the purpose and means of processing personal information (**Controller**):



**Data Processing Agreement (DPA):** Processing activities by a supplier on the Controller's behalf (**Processor**) shall be governed by a DPA between the Controller and Processor.



**Data Protection Assessment.** Controllers must conduct and document a data protection assessment for various high-risk processing activities.



**Privacy Notice:** Yes, a Controller must provide consumers with a privacy policy, including a list of required information.



**Universal Opt-out Mechanism:** None.

4. **Consumer Rights:** Subject to certain exceptions, a Tennessee consumer has the right to:



**Confirm** whether a Controller is processing their personal information and **accessing** the personal information;



**Correct** inaccuracies in the consumer's personal information;



**Delete** personal information provided by, or obtained about, the consumer (subject to certain exceptions);



**Obtain** a copy of the personal information that the consumer provided to the Controller in a portable and readily usable format; and



**Opt-out** of data processing for targeted advertising, sales of personal information, and profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

## 5. Enforcement and Penalties:



**Private Right of Action:** None.



**Penalties:** Up to \$7,500 per violation in civil penalties. If the court finds the Controller or Processor willfully or knowingly violated the act, the court may, in its discretion, award treble damages.



**Cure Period:** There is a 60-day cure period; unlike some states, this is a permanent cure period that does not have a cutoff date.



**Safe Harbor.** Controllers and Processors have an affirmative defense to violations if they create, maintain, and comply with a written privacy policy that reasonably conforms to the National Institute of Standards and Technology (NIST) privacy framework as well as other requirements.