PUBLICATION

T-Minus Two Months: Another State Enters the National Stage – Preparing for the Tennessee Information Protection Act

Authors: Matthew George White, Madison J. McMahan
May 14, 2025

Effective July 1, 2025, Tennessee enters the national privacy conversation with the Tennessee Information Protection Act (TIPA), becoming the latest state to enact a comprehensive consumer data privacy law. However, this isn't just a local concern. TIPA reaches beyond Tennessee's borders to any business that targets Tennessee consumers and meets certain thresholds.

If your company conducts business in Tennessee or offers products or services targeted to Tennessee residents, generates $25 million or more in annual revenue, and processes personal data from 175,000 or more consumers – or just 25,000 if half your revenue comes from selling data – TIPA applies. For these companies, compliance is not optional; TIPA imposes clear legal obligations that demand thoughtful planning and proactive execution. Here's what you need to know – and what you should be doing now to get ready.

TIPA: The Need-to-Know

- **Who's Covered?**
  For-profit businesses targeting Tennesseans that meet certain revenue and data thresholds. TIPA excludes certain entities, including non-profits, government entities, HIPAA-covered entities and business associates, insurance companies licensed under state law, and financial institutions already regulated under the Gramm-Leach-Bliley Act (GLBA).

- **Data Exemptions**
  Like most states, the new law does not cover employee data. There are several other categories of data also exempted from TIPA, including GLBA data, health records, scientific research data, consumer credit reporting data, personal motor vehicle records, insurance data, and data regulated by the Family Educational Rights and Privacy Act or the federal Farm Credit Act.

- **What Rights Do Consumers Have?**
  Tennesseans will soon have the right to access, correct, delete, and port their personal data – and to opt out of its sale, use for targeted ads, or profiling with significant effects.

- **What's "Sensitive" Data?**
  TIPA applies heightened standards to data categories that carry greater risks of harm: health, race, religion, geolocation, biometric identifiers, and information collected from children under age 13. Processing this type of data requires clear, affirmative consent.

- **No Private Lawsuits**
  Only the Tennessee Attorney General can enforce TIPA, but don't assume that limits your risk – penalties can reach $7,500 per violation, and up to triple that amount for willful violations.

Controller and Processor Duties: You're Either Holding the Steering Wheel or Riding Shotgun

Under TIPA, businesses fall into two roles, each with its own set of responsibilities:

- **Controllers** (those who decide the "why" and "how") must:
  - Limit data collection to what's necessary (data minimization).
  - Be transparent (publish a privacy notice).
  - Respect purpose limitations (don't repurpose data without consent).
  - Implement reasonable security safeguards.
  - Respond to consumer requests within 45 days (with one 45-day extension allowed).
- **Processors** (those who follow the controller's instructions) must:
  - Enter into contracts with clear processing instructions.
  - Assist controllers with consumer rights requests.
  - Flow down privacy requirements to any subcontractors.

Both roles must be ready to **show their work**, especially when it comes to high-risk activities, including handling sensitive data, engaging in profiling, or selling personal info. That means conducting **Data Protection Assessments** to evaluate and document the risks associated with those practices.

Time to Tune Up: Your Notices and Contracts May Need an Upgrade

TIPA emphasizes clarity in privacy notices and structure in vendor contracts. Your **privacy notice** must disclose the categories of personal data collected, why it was collected, how consumers can exercise their rights, whether that data is sold, and, if so, to whom. If personal data is sold or used for targeted advertising, consumers must be informed and given an opportunity to opt out.

On the contracting side, **data processing agreements** with vendors must include detailed processing instructions, clearly define the purpose and scope of the data use, and require confidentiality, cooperation, deletion rights, and downstream compliance from subcontractors.

In short: prioritize clear communication with customers and tight coordination with your vendors.

Building a Defense through Design: NIST

One of TIPA's unique features is its built-in safeguard: if your privacy program **reasonably conforms to the NIST Privacy Framework**, it may serve as an affirmative defense in an enforcement action. While not a guarantee of blanket immunity, this provision rewards organizations that prioritize proactive, well-documented governance.

What You Should Be Doing Now

TIPA compliance isn't a plug-and-play exercise – especially if your existing privacy program was built for the CCPA, GDPR, or another law. It diverges from other laws in key ways (such as its treatment of pseudonymous data) and deserves a tailored approach.

Here's where to start:

- Map your data flows and vendor relationships.
- Review and update your privacy notices and opt-out mechanisms.
- Assess your contracts with processors.
- Understand how your organization handles sensitive and children's data.
- Build a process for consumer requests and appeals.
- Document risk assessments tied to high-risk processing.

Two Months to Go – Let's Get You TIPA-Ready

With the July 1 deadline quickly approaching, now is the time to get your privacy house in order. Baker Donelson's team of privacy experts works with companies nationwide – and right here in Tennessee – to build and operationalize privacy programs that not only meet legal standards but also enhance customer trust.

Whether you need to assess your obligations under TIPA, update your privacy notice, vet vendor contracts, or create a user-friendly consumer rights and appeals process, we can help you create a TIPA compliance plan that's practical, defensible, and tailored to your organization's goals. Reach out to the authors or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team to get started.

TIPA is coming – we're here to make sure you're ready when it arrives.