LEWIS RICE **Tennessee Information Protection Act (TIPA)**

The TIPA (July 1, 2025) governs entities that control ("controllers") or process ("processors") and, as applicable, sell, the personal data of Tennessee residents, other than in the employment or business-to-business contexts ("consumers"). It also grants Tennessee residents certain rights with respect to their personal data.

Applicability

The TIPA applies to persons that conduct business in Tennessee or produce products or services that are targeted to consumers who are residents of the state, that exceed **$25 million** is revenue, and either and:

- During a calendar year, control or process the personal data of at least **175,000** consumers, or
- Derive over **50%** of their gross revenue from the sale of personal data and control or process the personal data at least **25,000** consumers.

Practical Application for Businesses

Consumer Rights:

(1) **Right to Access**: the right to confirm whether a controller is processing personal data and access such data.
(2) **Right to Delete**: the right to delete personal data concerning the consumer.
(3) **Right to Correct**: the right to correct inaccuracies in personal data concerning the consumer.
(4) **Right to Data Portability**: the right to obtain the personal data in, to the extent technically feasible, a portable, and, to the extent practicable, readily usable format that allows the consumer to transmit the data to another entity without impediment, where processing is by automated means.
(5) **Right to Opt-out**: the right to opt out of the processing of personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) certain profiling.

Controller Obligations:

- Publish a privacy notice that contains requisite details and is reasonably accessible, clear and meaningful.
- Act on consumer requests within **45 days**; provide notice of extensions and the appeals process as necessary.
- Obtain consent to collect sensitive data, including personal data of any consumers under **13**.
- Conduct and document an impact assessment for each processing activity that poses a "heightened risk of harm" to the consumer (e.g., selling personal data, processing sensitive data, or targeted advertising or profiling with certain foreseeable risks).
- Enter into binding data processing agreements with requisite limitations for third-party processors.

Recommendations for Controllers:

- Regularly update data maps to detail personal data collection, including sensitive data and targeted advertising.
- Train employees how to handle consumer inquiries and requests.
- Maintain clear and executable data retention policies and procedures that comply with the NIST privacy framework.

Penalties:

- The Tennessee Attorney General has the exclusive enforcement authority.
- There is a 60-day cure period to correct violations following notice from the Tennessee Attorney General.
- A business that (1) creates and maintains a written privacy program that complies with a NIST privacy framework, or a comparable framework; and (2) provides consumers the above Consumer Rights have an affirmative defense against a violation of TIPA.
- Penalties may include actual damages and fines up to **$7,500 per violation**.