Tennessee Information Protection Act (TIPA) Summary

On May 11, 2023, Governor Bill Lee (R) signed HB 1181, the "Tennessee Information Protection Act" (TIPA) into law. The Act's provisions take effect on July 1, 2025. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **Tennessee Information Protection Act (TIPA)** applies to persons conducting business in the state or producing products or services that are targeted to consumers who are residents of the state that make $25 million in annual revenue and that during a calendar year does either of the following: (a) controls or processes personal information of at least 175,000 consumers or (b) controls or processes personal information of at least 25,000 consumers and derives over 50% of gross revenue from the sale of personal information.
Covered Data	***"Personal information"***: information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal information" does not include information that is publicly available or de-identified or aggregate consumer information. ***"Sensitive data"***: personal information that includes: (a) racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (b) genetic or biometric data that is processed for the purpose of uniquely identifying a natural person; (c) the personal data collected from a known child; (d) precise geolocation data.
Key Definitions	***"Consent"***: a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal information relating to the consumer. "Consent" may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. ***"De-Identified Data"***: data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to that individual. ***"Pseudonymous Data"***: personal information that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable natural person. ***"Targeted Advertising"***: displaying advertisements to a consumer that is selected based on personal information obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. ***"Sale of Personal Information"***: the exchange of personal information for monetary or other valuable consideration by the controller to a third party. "Sale of personal information" does not include: (a) the disclosure of personal information to a processor that processes the personal data on behalf of the controller; (b) the disclosure of personal information to a third party for purposes of providing a product or service requested by the consumer; (c) the disclosure or transfer of personal information to an affiliate of the controller; (d) the disclosure of information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience; (e) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

Consumer Rights	● **Access:** A consumer has the right to confirm whether a controller is processing the consumer's personal information and to access such personal information. ● **Correction:** A consumer has the right to correct inaccuracies in the consumer’s personal information, taking into account the nature of the personal information and the purposes of the processing of the consumer’s personal information. ● **Deletion**: A consumer has the right to delete personal information provided by the consumer. ● **Portability:** A consumer has the right to obtain a copy of the consumer's personal information that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means. ● **Opt Out Rights**: A consumer has the right to opt out of the sale of personal data.
Business Obligations	● **Responding to Consumer Requests**: A controller shall respond to a consumer without undue delay, but in all cases within 45 days of receipt of a request. The response period may be extended once by 45 days when reasonably necessary, by informing the consumer of any such extension within the initial 45-day response period, together with the reason for the extension. A consumer has the right to a free response up to twice annually. The controller bears the burden of demonstrating the manifestly unfounded, excessive, repetitive, or technically unfeasible nature of any denied requests and may charge the consumer a reasonable fee to cover such administrative costs or decline to act on such requests. A controller shall establish a process for a consumer to appeal the controller’s refusal to take action on a request within a reasonable period of time after the consumer’s receipt of the decision. The appeal process shall be conspicuously available at no cost to the consumer and similar to the process for submitting requests to initiate action pursuant to this section. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken in response to the appeal and provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint. ● **Data Minimization**: A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed. ● **Avoid Secondary Use**: A controller shall not process personal data for purposes that are beyond what is reasonably necessary to and compatible with the disclosed purposes for which such personal information is processed, as disclosed to the consumer, unless the controller obtains the consumer’s consent. ● **Data Security**: A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal information. Such data security practices shall be appropriate to the volume and nature of the personal data at issue. ● **No Unlawful Discrimination:** A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against a consumer. A controller shall not discriminate against a consumer for exercising any consumer rights. ● **Transparency**: Upon receipt of an authenticated consumer request, a controller shall provide a consumer with a reasonably accessible, clear, and meaningful privacy notice that includes: (a) the categories of personal data processed by the controller; (b) the purpose for processing personal data; (c) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (d) the categories of personal data that the controller shares with third parties; (e) the categories of third parties with whom the controller shares personal data; (f) the right to opt out of the sale of personal information to third parties and the ability to request deletion or correction of certain personal information. ● **Purpose Specification:** A controller shall not process personal information for purposes other than those expressly listed unless otherwise allowed by this part. Personal information processed by a controller may be processed to the extent that the processing is: (a) reasonably necessary and proportionate and (b) adequate, relevant, and limited to what is necessary in relation to the specific

	listed purposes. ● **Disclosure**: A controller shall clearly and conspicuously disclose the sale of personal data to third parties or processing of personal information to third parties for targeted advertising in addition to the manner in which a consumer may exercise the right to opt out of such activity.
Data Protection Assessments	A controller shall conduct and document a data protection assessment for certain processing activities of consumer personal information. Data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by the safeguards that can be employed by the controller to reduce the risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer, must be factored into this assessment. The attorney general and reporter may request that a controller disclose a data protection assessment that is relevant to an investigation being conducted by the attorney general and reporter and the controller shall make assessment available. The attorney general and reporter may evaluate the assessment for compliance. Data protection assessments are confidential and not open to public inspection and copying.
Controller / Processor Distinction	● **A processor shall adhere to the instructions of a controller and assist the controller** in meeting its obligations under TIPA. A contract between a controller and a processor shall govern the processor's data processing procedures. The contract is binding and shall clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. ● The contract shall also include requirements that the processor shall: (a) ensure that each person processing personal information is subject to a duty of confidentiality; (b) delete or return all personal information to the controller as requested at the end of the provision of services, unless retention of the personal information is required by law; (c) make available to the controller all information in its possession necessary to demonstrate the processor's compliance with obligations; (d) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical organization measures in support of the obligations using an appropriate and accepted control standard or framework and assessment procedure for the assessments; a processor shall provide a report of each assessment upon controller request; and (e) engage a subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor.
Exceptions and Exemptions	● A controller may disclose pseudonymous data or de-identified data with an exercise of reasonable oversight to monitor compliance with any contractual commitments. ● TIPA shall not be construed to restrict a controller's or processor's ability to: (a) comply with laws; (b) comply with inquiries by government authorities; (c) cooperate with law-enforcement agencies; (d) prepare for and defend legal claims; (e) providing a product or service requested by a consumer; (f) protect interests essential for life or physical safety of the consumer; (g) prevent, detect and protect against security incidents; (h) engage in scientific or statistical research in the public interest; (i) assist third parties with the obligations of TIPA. ● Data exempt from TIPA includes: protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, any licensed insurance company, and COPPA.

Enforcement	● TIPA does not provide the basis for, or be subject to, a private right of action to violations of this Act. ● **Affirmative Defense - Voluntary Privacy Program**: a controller or processor has an **affirmative defense** to a cause of action for a violation of this Act if they (1) provide a person with the substantive rights required by the Act and (2) create, maintain, and comply with a written privacy policy that (a) reasonably conforms to the NIST privacy framework and (b) is updated reasonably to conform with the most recent NIST privacy framework within 2 years of its publication. ● **Right to Cure**: The attorney general and reporter shall have exclusive authority to enforce violations of TIPA and shall provide a controller or processor 60 days' written notice identifying specific provisions being violated. Any controller or processor that violates the Act is subject to an injunction and liable for a civil penalty of not more than $15,000 for each violation. There is no sunset specified for the right to cure.