Rhode Island Data Transparency and Privacy Protection Act Summary

On June 28, 2024, S.2500/H.7787, the "Rhode Island Data Transparency and Privacy Protection Act" became law without Gov. Daniel McKee's (D) signature. The law will become effective on January 1, 2026. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA)** applies to for-profit entities that produce products or services that are targeted to residents of the state and that during the preceding calendar year did any of the following: (i) controlled or processed the personal data of at least 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction, or (ii) controlled or processed the personal data of at least 10,000 consumers and derived more than 20% of their gross revenue from the sale of personal data.
Covered Data	"***Biometric data***": data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual. ***"Personal data":*** any information that is linked or reasonably linkable to an identified or identifiable individual and does not include de-identified data or publicly available information. **"*Precise geolocation data*"**: information derived from technology, including but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility. **"*Pseudonymous data":*** personal data that cannot be attributed to a specific individual without the use of additional information provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual. *Note: consumer rights outlined in the Act do not apply to pseudonymous data.* **"*Publicly available information*":** information that is lawfully made available through federal, state, or municipal government records or widely distributed media, or a controller has a reasonable basis to believe a customer has lawfully made available to the public. ***"Sensitive Data"***: personal data that includes data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, the processing of genetic or biometric data for the purpose of uniquely identifying an individual, personal data collected from a known child, or precise geolocation data.
Key Definitions	***"Consent"***: a clear, affirmative act signifying a customer has freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the customer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include acceptance of a general or broad term of use or similar document

	that contains descriptions of personal data processing along with other, unrelated information, hovering over, muting, pausing or closing a given piece of content, or agreement obtained through the use of dark patterns. ***"Dark Pattern":*** a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern". ***"De-Identified Data"***: data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual. ***"Targeted advertising"***: displaying advertisements to a customer where the advertisement is selected based on personal data obtained or inferred from that customer's activities over time and across nonaffiliated internet websites or online applications to predict such customer's preferences or interests. "Targeted advertising" does not include advertisements based on activities within a controller's own internet websites or online applications, advertisements based on the context of a customer's current search query, or current visit to an internet website or online application, advertisements directed to a customer in response to the customer's request for information or feedback, or processing personal data solely to measure or report advertising frequency, performance or reach. ***"Sale of personal data":*** the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include the disclosure of personal data to a processor that processes the personal data on behalf of the controller, the disclosure of personal data to a third party for purposes of providing a product or service requested by the customer, the disclosure or transfer of personal data to an affiliate of the controller, the disclosure of personal data where the customer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party, the disclosure of personal data that the customer:(i) intentionally made available to the general public via a channel of mass media; and(ii) did not restrict to a specific audience, or 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, or a proposed 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 customer has the right to confirm whether a controller is processing the customer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret **Correction/Deletion:** A customer has the right to correct inaccuracies in the customer's personal data and delete personal data provided by, or obtained about, the customer, taking into account the nature of the personal data and the purposes of the processing of the customer's personal data **Portability:** A customer has the right to obtain a copy of the customer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the customer to transmit the data to another controller without undue delay, where the processing is carried out by automated means; provided such controller shall not be required to reveal any trade secret. **Profiling:** A customer has the right to opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the customer.

	Revocation: A controller must provide consumers with a mechanism to grant and revoke consent where consent is required. Upon receipt of revocation, the controller shall suspend the processing of data as soon as is practicable. The controller must effectuate the revocation within 15 days of receipt of the customer's revocation request.
Business Obligations	**Data Security:** establish, implement, and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data shall not process sensitive data concerning a customer without obtaining customer consent and shall not process sensitive data of a known child unless consent is obtained and the information is processed in accordance with COPPA. **No Unlawful Discrimination:** A controller shall not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against customers. **Purpose Specification:** Personal data processed by a controller may be processed to the extent that such processing is reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. **Responding to Consumer Requests:** A controller must respond to a customer without undue delay, but not later than 45 days after receipt of the request. A controller may extend the response period by an additional 45 days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of the extension within the initial 45-day response period and of the reason for the extension. If a controller declines to act regarding the customer's request, the controller must inform the customer without undue delay, but not later than 45 days after the receipt of the request, of the justification for declining to act and instructions for how to appeal the decision. Information provided in response to a consumer request must be provided by a controller free of charge, once per customer during any 12-month period. If requests from a customer are manifestly unfounded, excessively or repetitive, the controller may charge the customer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request. **Third Parties:** A controller may sell consumer data to a third party, provided that the consumer has not opted-out of the sale of their data. If a controller does sell data to a third party, they must conduct a data protection assessment to ensure that consumers are shielded from a heightened risk of harm. **Transparency:** Any commercial website or internet service provider conducting business in Rhode Island must designate a controller. The Act does not specify the process or requirements for such designations. The controller must post a notice on their platform that identifies: • all categories of personal data collected on its website, • ***all third parties*** to whom the controller has sold or ***may sell*** consumers' personal identifiable information to, and • an active email address or other online mechanism that a consumer may use to contact the controller. It is unclear if any new subsequent third parties must be identified.
Data Protection Assessments	The RIDTPPA requires controllers to conduct and document a data protection assessment for each processing activity that presents a heightened risk of harm to a consumer, which includes: • The processing of personal data for the purposes of targeted advertising;

	• The sale of personal data; • The processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of unfair or deceptive treatment of, or unlawful disparate impact on, customers, financial, physical or reputational injury to customers, a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of customers, where such intrusion would be offensive to a reasonable person, or other substantial injury to customers; and • The processing of sensitive data. Notably, the Act does not specify what the assessment must include.
Controller / Processor Distinction and Responsibilities	***"Controller"*:** an individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data ***"Processor"*:** an individual who, or legal entity that processes personal data on behalf of a controller. Processors shall adhere to the instructions of a controller, and shall assist the controller in meeting the controller's obligations as outlined under the RIDTPPA. • A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and 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 require that the processor: • Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; • At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; • Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations of this chapter; • After providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and • 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 assess the processor's policies and technical and organizational measures in support of the obligations of this chapter, using an appropriate and accepted control standard of framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.
Exceptions and Exemptions	The RIDTPPA shall not be construed to restrict a controller's or processor's ability to: • Comply with federal, state or municipal ordinances or regulations, • Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities, • Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations,

	• Investigate, establish, exercise, prepare for or defend legal claims,
	• Provide a product or service specifically requested by a customer,
	• Perform under a contract to which a customer is a party, including fulfilling the terms of a written warranty,
	• Take steps at the request of a customer prior to entering into a contract,
	• Take immediate steps to protect an interest that is essential for the life or physical safety of the customer or another individual, and where the processing cannot be manifestly based on another legal basis,
	• Prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action,
	• Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine, whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller, the expected benefits of the research outweigh the privacy risks, and whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification,
	• Assist another controller, processor or third party with any of the obligations of this chapter,
	• Process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is:
	  ○ Subject to suitable and specific measures to safeguard the rights of the customer whose 8 personal data is being processed, and
	  ○ Under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.
	
	The RIDTPPA contains several exemptions including:
	• Data protected health information under the Health Insurance Portability and Accountability Act (HIPAA);
	• identifiable private information collected as part of human research pursuant to the good clinical practice guidelines;
	• the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a customer's creditworthiness, standing, capacity, or character to the extent such activity is regulated under the Fair Credit Reporting Act;
	• personal data collected, processed, sold, or disclosed in accordance with the Driver's Privacy Protection Act and the Family Educational Rights and Privacy Act; and
	• data processed or maintained in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role.
	
	The RIDTPPA also includes an exemption for any state body, non-profit organization, or data subject to the Gramm-Leach-Bliley Act.

Enforcement	The Attorney General has sole enforcement authority over provisions in the Act and does not include provisions allowing for a right to cure. A violation of the Act shall constitute a deceptive trade practice; provided, further, that in the event that any individual or entity intentionally disclose personal data: (1) To a shell company or any entity that has been formed or established solely, or in part, for the purposes of circumventing the intent of this chapter; or

	(2) In violation of any provision of this chapter, that individual or entity shall pay a fine of not less than one hundred dollars ($100) and no more than five hundred dollars ($500) for each such disclosure.