Articles + Publications | July 1, 2024

Rhode Island Adds to the Growing Patchwork of State Privacy Laws – H7787 / S2500

WRITTEN BY

Kim Phan | Laura Hamady | Natasha E. Halloran

Rhode Island has become the 19th U.S. state to enact a comprehensive privacy law. On June 25, Rhode Island Governor Daniel McKee (D) transmitted the Rhode Island Data Transparency and Privacy Protection Act (RI-DTPPA) into law without signature. The RI-DTPPA contains similar business obligations and consumer rights as other state privacy laws. The RI-DTPPA will take effect on January 1, 2026, and the state attorney general (AG) will have sole enforcement authority.

Applicability

The RI-DTPPA applies to for-profit entities that conduct business in Rhode Island or produce products or services targeted to Rhode Island residents and that, during the preceding calendar year, satisfy any of the following:

1. Controlled or processed the personal data of not less than 35,000 customers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

2. Controlled or processed the personal data of not less than 10,000 customers and derived more than 20% of their gross revenue from the sale of personal data.

Exemptions

The RI-DTPPA provides several exemptions, including both entity-level and data-level exemptions, and an exemption for processing personal data to comply with law enforcement investigations.

The entity-level exemptions include state agencies, nonprofit organizations, higher education institutions, financial institutions subject to the Gramm-Leach-Bliley Act (GLBA), and covered entities or business associates regulated by the Health Insurance Portability and Accountability Act (HIPAA).

Categories of data-level exemptions include data regulated by HIPAA, federal research laws, the Fair Credit Reporting Act, the GLBA, the Driver's Privacy Protection Act, the Family Educational Rights and Privacy Act, and the Farm Credit Act, among others.

Rhode Island also includes employee and business-level exemptions. A "customer" is defined as an individual

©2026 Troutman Pepper Locke

residing in the state acting in an individual or household context and exempts an “individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual’s role with the company, partnership, sole proprietorship, nonprofit or government agency.”

Customer Rights

The RI-DTPPA provides for the typical set of consumer rights described in other state privacy laws, including the right to access, right to correct, right to delete, right to obtain copies of their personal data, and right to opt out of processing for targeted advertising, sales of personal data, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the customer, and right to designate an authorized agent. The consumer rights offered under RI-DTPPA do not extend to pseudonymous data where the “where the controller is able to demonstrate that any information necessary to identify the customer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information[,]” potentially offering regulated entities an incentive to invest more heavily in this type of data security.

Like other states, controllers are allocated 45 days to respond to customer requests and may deny certain requests, for example, due to the controller’s inability to authenticate a request.

Controllers must offer customers the ability to appeal any denial of a consumer request to exercise their rights. The RI-DTPPA provides additional details about how the appeal process should work, including that it should be “clearly and conspicuously” available to customers. Specifically, not later than 60 days after receipt of an appeal, a controller must inform the customer in writing of any action taken or not taken, including a written explanation of the reasons for the controller’s decision. The customer is permitted to submit a complaint to the state AG if the appeal is denied.

Controller and Processor Obligations

Controller and processor obligations under the RI-DTPPA are similar to those ascribed in other state privacy laws with some variations. Obligations under the RI-DTPPA include, but are not limited to:

- Establishing, implementing, and maintaining reasonable administrative, technical, and physical data security practices;
- Obtaining consent to process sensitive data and creating a mechanism for customers to grant and revoke consent. Controllers have up to 15 days to effectuate revocation of a customer’s consent;
- Entering into a contract to govern the processor’s procedures with respect to processing on behalf of the controller and setting forth certain data processing terms and confidentiality requirements;
- Conducting data protection assessments for each of the controller’s high-risk processing activities such as the processing of personal data for the purposes of targeting advertising, the sale of personal data, processing for

profiling purposes, and processing of sensitive data. Data protection assessment requirements apply to processing activities created or generated after January 1, 2026, and are not retroactive; and

- Providing customers with a privacy notice that includes categories of personal data collected, third parties it has sold or may sell customers' personally identifiable data, and an active email or other online mechanism that the customer may use to contact the controller. Notably, if a controller sells personal data or processes personal data for targeted advertising purposes, it must "clearly and conspicuously" disclose that processing.

Additionally, any controller in possession of de-identified data must take reasonable measures to ensure that the data cannot be associated with an individual, publicly commit to maintaining and using de-identified data without attempting to re-identify the data, and contractually obligate any recipients of the de-identified data to comply with the RI-DTPPA.

Enforcement

There is no private right of action. The Rhode Island AG has sole enforcement authority. A violation of the RI-DTPPA constitutes a violation of Rhode Island's general regulatory provisions of commercial law and a deceptive trade practice in violation of Rhode Island law. In certain circumstances, the RI-DTPPA authorizes a fine of $100 to $500 for each intentional disclosure.

Practice Tips

To prepare for the RI-DTPPA's effective date, companies should assess whether they meet the RI-DTPPA's threshold and whether one of the distinct controller obligations may apply to their business. Specifically, if applicable, a company should ensure it has mechanisms to obtain opt-in consent for the processing of sensitive data and effectuate revocation requests, mechanisms to effectuate customer opt outs, and conduct data protection assessments for high-risk processing activities.

Further, there are also statutory ambiguities that companies will likely have to grapple with before the January 1, 2026, effective date. For example, in the information sharing practices section, the RI-DTPPA alternates between the use of "personal data" and "personally identifiable information," the latter term which is undefined. The varying terms could mean that there are two distinct categories of data to consider in the privacy notice, or it could be a drafting oversight where the two terms should be interpreted to mean the same thing.

Additionally, companies should be aware that the RI-DTPPA poses heightened noncompliance exposure due to the inability to cure noncompliance deficiencies. Specifically, the RI-DTPPA does not provide a cure provision to alert companies of alleged violations and provide an opportunity to correct such noncompliant data practices. Further, the state AG has the authority to penalize companies $100 to $500 for each intentional violation of the RI-DTPPA. Thus, the inability to cure and possible statutory penalties for each intentional violation mean companies should carefully review their data practices as they relate to compliance with Rhode Island.

Troutman Pepper will continue to monitor the RI-DTPPA as well as all other data privacy law developments.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber