CLIENT ALERT: Rhode Island's Comprehensive Data Privacy Law Takes Effect January 1, 2026: Compliance Overview for Businesses

By Spencer Bogle *April 29, 2025*

On June 28, 2024, Rhode Island enacted the Rhode Island Data Transparency and Privacy Protection Act (the "Act"), joining nineteen other states in the U.S. with comprehensive data privacy legislation. Effective January 1, 2026, the law will affect many New England businesses due to the ubiquity of online commerce and New England's interconnected economy. While the Act follows the framework of similar data privacy laws enacted in other U.S. states, entities doing business in Rhode Island should review the Act to ensure compliance.

Key Terms and Framework

Similar to other states' data privacy laws, the Act defines "personal data" as any information that is linked or reasonably linkable to an identified or identifiable individual, excluding de-identified data or publicly available information. Also like other states' data privacy laws, "processing" refers to the collection, use, storage, analysis, deletion, or modification of personal data, or any other "operation or set of operations performed" on personal data.

The Act imposes obligations on both controllers and processors. A "controller" is the individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data. A "processor" is an individual who, or legal entity that, processes personal data on behalf of the controller. While the Act requires both controllers and processors to implement compliance procedures, controllers are charged with the responsibility to carry out most of the Act's mandates.

The Act delineates two types of obligations, the first requires the transparent disclosure of certain personal data use to Rhode Island residents and the second requires the implementation of procedures that protect Rhode Island residents' personal data.

Data Sellers – Transparency Obligations

Commercial websites and ISPs which conduct business in Rhode Island, have customers in Rhode Island, or are otherwise subject to Rhode Island's jurisdiction must designate a controller. Commercial websites and ISPs that collect, store and sell personally identifiable information to third parties must, in a customer agreement or incorporated addendum, or in another conspicuous location on their website or online service platform where similar notices are posted, identify:

- All categories of personal data that the controller collects through the website or online services about customers;
- All third parties to whom the controller has sold or *may sell* customers' personally identifiable information; and
- All active email addresses or other online mechanisms that customers may use to contact the controller.

Additionally, controllers that sell personal data to third parties or that process personal data for targeted advertising must disclose such activity clearly and conspicuously.

Control or Processing Thresholds – Privacy Protection Obligations

A for-profit entity that conducts business in Rhode Island or produces products or services targeted at Rhode Island residents is subject to the Act's data protection obligations if, during the preceding calendar year, it:

(1) controlled or processed personal data of at least 35,000 Rhode Island residents, excluding personal data controlled or processed *solely* for purposes of completing payment transactions, or
(2) controlled or processed personal data of 10,000 or more Rhode Island residents and derived 20% of its gross revenue from the sale of personal data.

Such entities shall be referred to herein as "Threshold Controllers/Processers."

These thresholds are lower than those in other states' data privacy laws, likely reflecting Rhode Island's lower population.

Excluded Entities and Categories of Personal Data

The Act does not apply to state or local government entities or subdivisions, nonprofits, higher education institutions, national securities associations registered under the Securities Exchange Act of 1934, financial institutions subject to the Gramm-Leach-Bliley Act, or covered entities or business associates under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Certain categories of personal data are also exempt. Personal data that is already subject to strict regulations, such as protected health information subject to HIPAA, information collected for use in a customer report that is regulated and authorized by the Fair Credit Reporting Act, and personal data subject to Family Educational Rights and Privacy Act, is exempt. Furthermore, personal data processed in the employment context, such as from an individual applying to, being employed by, or acting as an agent or independent contractor of, a for-profit business, and data processed in commercial (business-to-business) context is also exempt.

Personal Data Protection Rights

Threshold Controllers/Processors must implement procedures to allow Rhode Island residents to exercise control over the processing of their personal data. As to personal data processed by Threshold Controllers/Processors, a Rhode Island resident has the right to:

- **Confirm** whether a controller is processing his or her personal data and access such personal data, unless confirmation requires disclosure of a trade secret;
- **Obtain** a copy of his or her personal data, to the extent technically feasible, in a readily usable format – provided such controller is not required to reveal any trade secret;
- **Correct** inaccuracies in his or her personal data;
- **Delete** his or her personal data; and
- **Opt out** of the processing of his or her personal data for the purposes of targeted advertising, the sale of personal data, or profiling.

Controllers may not discriminate against a Rhode Island resident who exercises his or her rights, nor may they deny goods or services, charge different prices or rates for goods or services, or provide a different level of quality of goods or services if that resident opts out of the processing of his or her personal data. If a Rhode Island resident opts out, the business is not required to provide products or services that require the collection of that resident's personal data.

A customer may exercise his or her personal data rights by "secure and reliable means established by the controller and described to the customer in the controller's privacy notice."

Controllers must also comply with a request by a Rhode Island resident to exercise his or her data privacy rights within 45 days of the request's receipt, which can be extended by an additional 45 days so long as the controller informs the resident of the extension within the initial 45-day period. The controller must process a resident's request free of charge once per 12-month period. If the controller deems a resident's request to be

"manifestly unfounded, excessive, or repetitive," the controller must demonstrate why it is so to decline to act on the request or to charge a reasonable fee for subsequent requests. If the controller declines to act on a Rhode Island resident's request, it must inform that resident of its reasons within 45-days of receiving the request.

Controllers must also create and administer an appeal process for denials. This appeal process must be clearly and conspicuously available, and controllers must provide Rhode Island residents with an appeal decision, including a written explanation justifying the decision, within 60 days of receiving the appeal request. If the appeal is denied, the Rhode Island resident may submit a complaint to the Rhode Island Attorney General.

If a controller is unable to authenticate a Rhode Island resident's request to exercise his or her rights, the controller is not required to comply with the request. However, the controller must inform the Rhode Island resident that it is unable to authenticate the request until that resident provides additional information that is reasonably necessary to authenticate the resident and his or her request. A controller is not obligated to authenticate opt-out requests but may deny an opt-out request if it has reasonable and documented belief that the request is fraudulent and provides notice to the requestor that the controller believes the request is fraudulent, the reasons for that belief, and that it will not comply with the request.

Personal Data Protection Obligations on Controllers

To comply with the Act's privacy protection obligations on Threshold Controllers/Processors, controllers must:

- Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data;
- Obtain a Rhode Island resident's consent prior to processing "sensitive data" – data revealing an individual's 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 known individual under the age of 18, or precise geolocation data;
- Obtain verifiable parental consent, as defined in the Children's Online Privacy Protection Act of 1998, to process a known child's sensitive data;
- Conduct and document a data protection assessment for each controller activity that presents a heightened risk of harm, such as processing personal data for targeted advertising, selling personal data, processing sensitive data, or processing personal data for the purpose of profiling (if the 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 private affairs or concerns," of customers);
- Process data in a non-discriminatory way as defined under state and federal law prohibiting unlawful discrimination against Rhode Island residents; and
- Provide Rhode Island residents with a mechanism to grant and revoke consent – where consent is required – and suspend the processing of a Rhode Island resident's personal data after he or she revokes consent no later than 15 days from receipt of the revocation.

Under the Act, Threshold Controllers/Processors may process personal data to the extent that is reasonably necessary in relation to the disclosed and lawful purpose for which said personal data is processed.

Personal Data Protection Obligations on Processors

The Act's obligations on Threshold Controllers/Processors also regulate processors which must adhere to their controllers' instructions and assist their controllers in meeting

their controllers' obligations. Furthermore, a processor may become a controller if it begins to determine the purposes and means of processing personal data.

Contracts between Controllers and Processors

Finally, the Act's obligations on Threshold Controllers/Processors regulate contracts between controllers and processors. Contracts between controllers and processors must 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. These contracts must also require that the processor:

- Ensure that each person processing personal data is subject to a duty of confidentiality with respect to such data;
- Delete or return all personal data to the controller at the end of the provision of services, unless retention of the data is required by law;
- Provide information to the controller which demonstrates the processor's compliance with the Act;
- Provide the controller with an opportunity to object to the processor's engagement with a subcontractor; and
- Allow, and cooperate with, a reasonable assessment by the controller, or to arrange an assessment by an independent assessor of the processor's choosing, to audit the processor's ability to comply with the Act.

Like other states' data privacy laws, controllers and processors that comply with the Act's obligations on Threshold Controllers/Processors are not responsible for violations committed by processors or third-party controllers to whom they properly transmit personal data, unless they had actual knowledge when the transfer was made that the processor or third-party would break the law. Similarly, third parties who receive personal data from a controller or processor are not responsible for violations by the party from whom the third party received the personal data.

Enforcement of the Act

The Rhode Island Attorney General has exclusive authority to enforce the Act. There is no private right of action. Each violation of the Act constitutes a deceptive trade practice, carrying a penalty of up to $10,000 for each violation. Furthermore, an individual or entity that intentionally discloses personal data is subject to a fine of a minimum of $100 and a maximum of $500 for each violation. *Unlike other states' data privacy laws, the Act does not provide a right to cure violations*.

RECOMMENDATIONS

- Conduct an audit to determine whether Act applies to the business by determining: (1) whether the business sells personally identifiable information; (2) whether the business processes the personal data of enough Rhode Island residents to trigger the Act's obligations on Threshold Controllers/Processors; (3) whether the data collected by the business is exempt from the Act's obligations; (4) whether the data is sensitive data; and (5) how the personal data is used.
- Create a privacy notice that conforms to the business' obligations under the Act and post it in a prominent and conspicuous place that Rhode Island residents can easily access.
- For commercial websites and ISPs subject to the Act as data sellers, designate a controller.
- For for-profit entities subject to the Act's obligations on Threshold Controllers/Processors, create, implement and monitor compliant procedures to: (1) correctly process personal data; (2) handle requests by Rhode Island residents to control their personal data; (3) limit the processing of personal data to that which is necessary; and (4) establish compliant contractual relationships with processors.

***

Copyright © 2025 Belcher Fitzgerald LLP.
All rights reserved.
This publication is not intended as legal advice. Before you make any decision that may have legal implications, you should consult with a qualified legal professional for specific legal advice.

101 FEDERAL STREET, SUITE 705 • BOSTON, MA 02110
PHONE: 617.368.6890 • FAX: 617.368.6891
www.belcherfitzgerald.com