Now & Next
Healthcare & Privacy Alert

July 26, 2024

Rhode Island enacts data privacy law

By **Meredith LaMaster** and **Julia Cassidy**

The Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA) outlines how businesses must protect customer data.

What's the impact?

- While similar in many respects to other recently enacted comprehensive privacy acts, RIDTPPA privacy notice applicability and disclosure requirements exceed those seen in other states.
- Businesses serving Rhode Island residents will need to evaluate their privacy practices to make necessary adjustments to comply with RIDTPPA's opt-out and applicability requirements.

On June 28, 2024, Rhode Island became the nineteenth state to enact a data privacy law, joining California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia. The law focuses on providing customers with transparency with regard to how their personally identifiable information (PII), particularly that of children, is used and shared by data controllers and processors. RIDTPPA goes into effect on January 1, 2026.

Definitions under RIDTPPA

CONTROLLER

An individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data.

COVERED ENTITY

A health plan, a healthcare clearinghouse, or a healthcare provider who transmits any health information in electronic form in connection with a standard transaction.

CUSTOMER

An individual residing in this state acting in an individual or household context. "Customer" does not include 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.

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.

PROCESS OR PROCESSING

Any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

PROCESSOR

An individual who, or legal entity that, processes personal data on behalf of a controller.

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.

Information sharing practices

Under RIDTPPA, any commercial websites or internet service providers (ISP) transacting business in Rhode Island, with Rhode Island customers, or that otherwise fall under Rhode Island's jurisdiction, must designate a controller. If that website or ISP collects, maintains, and sells customers' PII, then the controller must identify:

- The categories of customers' personal data collected through the website or online service;
- Third parties that customers' PII has been sold to or may be told to; and
- An active email address or other online communication platform that can be utilized to contact the controller.

This information can be included in the controller's customer agreement, or in another clear and easily locatable location on its website or online service platform. If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose the processing.

This section of the RIDTPPA also includes an extended list of entities and types of information that are exempt and differs in some respects from the entities discussed below in "RIDTPPA exemptions." Entities and types of information that are exempt include:

- Any Rhode Island body, authority, board, bureau, commission, district, agency, or political subdivision;
- Nonprofit organizations;
- Higher education institutions;
- National securities associations registered under the Securities Exchange Act of 1934;
- Financial institution or data subject to Title V of the Gramm-Leach-Bliley Act;
- Covered entities or business associates, as defined under HIPAA;
- Protected health information or de-identified information, as defined under HIPAA;
- Patient-identifying information for purposes of mental health and substance abuse records;
- Identifiable private information for the protection of human research subjects;
- Identifiable private information collected as part of human subjects' research under the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;
- The protection of human subjects, or personal data used or shared in research, or other research conducted in accordance with applicable law;
- Information and documents created for the Health Care Quality Improvement Act of 1986;
- Patient safety work product for the Patient Safety and Quality Improvement Act;

- Information derived from and intermixed to be indistinguishable with, or information treated in the same manner as, exempt information that is maintained by a covered entity or business associate, program, or qualified service organization;
- Public health activity information authorized by HIPAA, community health activities, and population health activities;
- The collection, maintenance, disclosure, sale, communication, or use of any personal information regulated under the Fair Credit Reporting Act;
- Personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994;
- Personal data regulated by the Family Educational Rights and Privacy Act;
- Personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act;
- Data processed or maintained by an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, as the emergency contact information of an individual or that is needed to administer benefits for another individual relating to the individual who is the subject of the information and used to administer benefits; and
- Personal data collected, processed, sold, or disclosed in relation to price, route, or service, as used in the Airline Deregulation Act, by an air carrier subject to said act.

RIDTPPA applicability

RIDTPPA applies to for-profit entities conducting business in Rhode Island or for-profit entities that produce products or services targeted to Rhode Island residents and that in the prior calendar year participated in any of the following:

- Controlled or processed the personal data of 35,000 or more consumers, with the exception of personal data controlled or processed solely to effectuate payment or
- Controlled or processed the personal data of 10,000 or more consumers, in addition to obtaining at least twenty percent (20%) of gross revenue from personal data sales.

These applicability thresholds mimic those established in the Maryland Online Data Privacy Act (MODPA). As discussed in our MODPA alert, twenty percent (20%) is a lower revenue threshold than what is seen in many other states, which will increase the number of businesses required to comply with RIDTPPA. RIDTPPA also applies to covered entities that opt to collect, store, and sell or otherwise transfer or disclose PII. Although the term PII is used throughout RIDTPPA, it is never defined, which brings about questions as to how widely applicable certain parts of the Act are.

RIDTPPA exemptions

RIDTPPA is not applicable to:

- Contractors, subcontractors, or agents of state agencies or local units of government when working in such capacity.
- Financial institutions and their affiliates subject to the Gramm-Leach-Bliley Act (GLBA).
- Information or data subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Recognized tax-exempt organization under the Internal Revenue Code.

In addition to these exempt entities, RIDTPPA does not regulate certain types of data and information, including the retention or disclosure of an individual's PII, nor does it prohibit or restrict the distribution or sale of product sales summaries or statistical information or aggregate customer data, which may include PII. RIDTPPA also does not apply to PII, or any other information collected, used, processed, or disclosed by or for a customer reporting agency. Entities are not required to collect, store, or sell PII, nor are controllers required to offer a good or service that requires personal data not collected or maintained by the controller. The requirements imposed on controllers or processors will not apply when compliance would violate evidentiary privilege under Rhode Island law. Controllers or processors are permitted to provide customers' personal data to a person covered by evidentiary privilege as part of a privileged communication.

Obligations imposed on controllers and processors

Processing of information: Controllers must develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of personal data. To process customers' sensitive data, controllers must obtain consent. With respect to the sensitive data of known minors, processors are required to attain parental consent and must process data in compliance with the Children's Online Privacy Protection Act (COPPA).

Controller and processor responsibilities: A processor must follow the instructions of a controller and assist the controller in meeting the controller's obligations. A contract between the parties will govern the processor's data processing procedures for services performed on behalf of the controller. The contract will be binding and clearly set forth instructions for processing data, the scope and purpose of processing, the type of data subject to processing, the length of processing and the rights and obligations of both parties. A controller must conduct and document a data protection assessment for each processing activity that presents a heightened risk of harm to a customer. Activities that present a heightened risk of harm to a customer include: (1) processing personal data for targeted advertising; (2) the sale of personal data; (3)

processing personal data for profiling purposes, where the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment of, or unlawful disparate impact on, customers, financial, physical or reputational injury, a physical or other offensive intrusion upon the solitude or seclusion, or the private affairs or concerns, of customers, or other substantial injury to customers; and (4) processing of sensitive data.

Customer rights

Controllers are prohibited from discriminating against customers for exercising their customer rights. Controllers cannot deny goods or services, charge different rates, or provide a different quality level of goods or services to customers for opting out. If a customer opts out, a covered entity is not required to provide a service that mandates the data collection. It is permissible for controllers to set different prices and levels for goods and services for a bona fide loyalty, rewards, premium features, discount, or club card programs that customers voluntarily participate in.

Customers have the right to:

- Confirm whether a controller is processing customers' personal data and accessing that personal data, unless it would require the controller to reveal a trade secret;
- Correct discrepancies, and delete personal data provided by, or acquired about, the customer, dependent upon the scope of the data and the reasons for processing;
- Acquire a copy of the processed personal data, in a portable and readily usable format that allows the customer to transmit the data to another controller without undue delay, where the processing is conducted by automated means, as long as the controller isn't required to reveal any trade secret; and
- Opt out of personal data processing for targeted advertising, the sale of personal data, or profiling for solely automated decisions that produce legal or similarly significant effects.

EXERCISING CUSTOMER RIGHTS

Controllers must comply with customer requests to exercise their authorized rights as follows:

- Respond without undue delay, but no later than forty-five (45) days after receiving a request. Response periods can be extended by forty-five (45) more days when reasonably necessary.
- Information provided in response to a customer request must be free of charge, once per customer during any twelve (12) month period.
- A controller that has obtained personal data from a third party will be deemed in compliance with a customer's deletion request by: (i) Retaining a record of the request and the minimum data necessary to ensure the personal data remains deleted from the controller's records and

not using retained data for any other purpose; or (ii) Opting the customer out of the processing of personal data for any reason except for those exempted.

- A controller must establish a clear and conspicuous customer appeal process for refusal to act on a request within a reasonable period after receipt of the decision.

Enforcement

The Rhode Island attorney general has sole enforcement authority of RIDTPPA. Violations of RIDTPPA constitute deceptive trade practices. If any individual or entity intentionally discloses personal data: (1) To a shell company or any entity that has been formed or established solely, or in part, to evade RIDTPPA; or (2) In violation of RIDTPPA, they may be fined between one hundred dollars ($100) and five hundred dollars ($500) for each disclosure. Private rights of actions are not allowed under RITPDDA, nor is a cure period for non-compliance by entities discussed.

Businesses must prioritize data privacy compliance

While RIDTPPA is likely to undergo future amendments to tie up loose ends, its general structure aligns with many of the comprehensive data privacy acts recently enacted. Accordingly, businesses offering goods and services to Rhode Island residents will need to evaluate their business and privacy practices on an ongoing basis to ensure they align with state requirements.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Meredith D. LaMaster
312.977.9257
mlamaster@nixonpeabody.com

Julia E. Cassidy
212.940.3137
jcassidy@nixonpeabody.com