THOMPSON HINE

Privacy & Cybersecurity Update

July 2024

Rhode Island Enacts Consumer Data Privacy Law

On June 25, the Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA) entered into force. The RIDTPPA furnishes Rhode Island residents with several data protection rights and requires covered businesses to comply with new data privacy and information security requirements. The RIDTPPA does *not* create a private right of action and delegates sole enforcement authority to the Rhode Island attorney general. The law becomes effective on January 1, 2026.

Scope of Applicability

The RIDTPPA generally applies to for-profit organizations that conduct business in Rhode Island or produce products or services targeted to residents in the state and do any of the following during a calendar year:

- control or process personal data of at least 35,000 consumers (excluding personal data processing for payment transactions) *or*
- control or process the personal data of at least 10,000 customers and derive more than 20% of gross revenue from the sale of personal data.

The RIDTPPA includes several standard exemptions typically found in data privacy frameworks, such as exemptions for state and local governments, organizations governed by federal laws like HIPAA, GLBA, and FERPA, nonprofit organizations, and air carriers subject to the federal Airline Deregulation Act, among others.

Key Terms

The RIDTPPA primarily regulates how data "controllers" and "processors" collect and process a consumer's personal data. A "consumer," is defined as any Rhode Island resident acting in an "individual or household context." The term generally excludes personal data concerning individuals acting in a commercial or employment capacity, HR data and personal data related to job applicants. The RIDTPPA also excludes "de-identified data" or "publicly available information," each of which has its own definition under the law.

The RIDTPPA establishes additional requirements for processing "sensitive data," defined as a subset of personal data including: (i) information revealing racial or ethnic origin, religious beliefs, mental or physical health conditions or diagnoses, sex life, sexual orientation, or citizenship or immigration status, (ii) processing biometric data or genetic information used to uniquely identify an individual, (iii) the personal data of a known child, or (iv) precise geolocation data.

Consumer Privacy Rights and Appeals

As with other state privacy laws, the RIDTPPA grants consumers the right to:

- Confirm whether a controller is processing personal data concerning the consumer and access the categories of personal data the controller is processing.
- Correct inaccuracies in the customer's personal data and delete personal data provided by, or obtained about, the customer, considering the nature of the personal data and the purposes of the processing of the personal data.
- Obtain personal data concerning the consumer, which they previously provided to the controller, in a portable

> and, to the extent technically feasible, readily usable format that allows them to transmit the data to another controller without undue delay, where the processing is carried out by automated means.

The law mandates that customers can exercise their rights through secure and reliable means established by the controller and detailed in the controller's privacy notice. The RIDTPPA requires controllers to set up procedures for receiving, processing, and responding to data privacy requests, including authenticating consumer requests and adhering to specific response timelines. Additionally, controllers must create a framework for consumers to appeal decisions regarding their privacy requests. When informing a consumer of any action taken or not taken in response to an appeal, the controller must provide a written explanation of their decision. If a privacy request is denied, the law permits the consumer to file a complaint with the state's attorney general, though it does not require controllers to provide this information.

Opt-Out Rights - Targeted Advertising and Sales

In addition to the rights previously mentioned, the RIDTPPA grants consumers the right to opt out of personal data processing for targeted advertising, sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the customer.

The term "targeted advertising" means "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests." However, as with the definition of "sale of personal data," the definition of "targeted advertising" includes several exceptions within its meaning that are common across other U.S. state data protection laws.

Similarly, the RIDTPPA's definition of the "sale of personal data" is like that found in other U.S. state data protection laws which means "the exchange of personal data for monetary or other valuable consideration by the controller to a third party." However, several activities are excluded from its scope, such as:

- the disclosure of personal data to a processor (e.g., service provider),
- the disclosure of personal data to a third-party for purposes of providing a product or service requested by the consumer,
- 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,
- the disclosure of personal data where the customer intentionally uses the controller to interact with a third party,
- 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, or
- the disclosure or transfer of personal data to a third party as an asset that is part of a corporate restructuring or bankruptcy.

A consumer may designate another person as the consumer's authorized agent to exercise the consumer's right to opt out of the processing of the consumer's personal data for purposes of targeted advertising and sale. In turn, a controller must honor an opt-out request from an authorized agent if the controller can verify the consumer's identity and the agent's authority to act on the consumer's behalf.

Controller Obligations, Consent

A controller processing personal data must be reasonably necessary regarding the purposes for which such data processed as disclosed to the consumer, adequate, relevant, and limited to what is essential concerning a specific purpose. Further, a controller may not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of personal data concerning a known child, without obtaining consent from the child's parent or lawful guardian. A controller must "provide a mechanism for individuals to grant and revoke their consent, where consent is required." If a consumer's consent is revoked, then a controller must

suspend its data processing as soon as practicable, but not later than 15 days after receiving the request.

Privacy Notices

Under the RIDTPPA, a controller that collects, stores, and sells customers' personally identifiable information must make certain disclosures. For instance, a controller must address in its customer agreement, addendum, or in another conspicuous location on its website or online service platform where similar notices are customarily posted the following:

- Identify all categories of personal data that the controller collects through the website or online service about customers,
- Identify all third parties to whom the controller has sold or may sell customers' personally identifiable information, and
- Identify an active electronic mail address or other online mechanism the customer may use to contact the controller.

Moreover, if a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose such processing.

Information Security and Data Protection Assessments

The RIDTPPA requires a controller to "establish, implement, and maintain reasonable administrative, technical, and physical data security practices" to protect the confidentiality, integrity, and accessibility of personal data.

Additionally, under the RIDTPPA, a controller must conduct and document a protection assessment for each processing activity that presents a heightened risk of harm to a customer and more specifically:

- the processing of personal data for targeted advertising purposes,
- the sale of personal data,
- the processing of sensitive data,
- the processing of personal data for purposes of profiling, where the profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (ii) financial, physical, or reputational injury to consumers, (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person, or (iv) other substantial injury to consumers.

Data privacy and protection assessments, or risk assessments conducted by a controller for compliance with other laws or regulations, may qualify under this section if they have a similar scope and effect. A single assessment can address multiple sets of comparable processing operations encompassing similar activities. The law permits the state's attorney general to request these assessments and requires the controller to disclose them under certain conditions, provided the confidentiality of the assessment is preserved.

Processor Obligations and Data Processing Agreements

The RIDTPPA places affirmative obligations on processors, including "adhering to the instructions of the controller" and "assisting the controller to meet" its legal obligations. It requires controllers and processors to execute agreements (often called "data processing agreements") that 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. Per the terms of these contracts, a processor must: (i) ensure the confidentiality of its personnel concerning the data, (ii) engage subcontractors only with the controller's approval and under the same data processing terms and conditions, (iii) agree to audits, compliance, and inspection provisions, and (iv) delete or return the controller's personal data at the end of the service provision.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Thora Knight, Ph.D.
212.908.3971
Thora.Knight@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)