HINSHAW

Is Your Business Prepared to Comply With Rhode Island's Comprehensive Privacy Law?

Privacy, Cyber & AI Decoded Alert | 4 min read
Jul 15, 2024

Rhode Island is the latest state to enact consumer privacy legislation. The Rhode Island Transparency and Privacy Protection Act (the "Act"), which passed into law on June 28, 2024, establishes a framework for controlling and processing personal data and includes consumer rights similar to those of other existing state laws. The Act goes into effect on **January 1, 2026**.

Who Does the Act Apply to?

The Act applies to "controllers" that conduct business in Rhode Island or produce products or services that are targeted to residents of Rhode Island that:

- Controlled or processed personal data of at least 35,000 Rhode Island customers, excluding instances where controllers are processing data "solely for the purpose of completing a financial transaction;" or
- Controlled or processed personal data of 10,000 Rhode Island customers and derived more than 20 percent of their gross revenue from the sale of personal data.

"Controller" is defined as "an individual who, or legal entity that, alone or jointly with others, determines the purpose and means of processing personal data."

"Processor" is defined as "an individual who, or legal entity that, processes personal data on behalf of a controller."

The Act will **not** apply to:

- State and local government entities;
- Non-profits and other tax-exempt organizations;
- Institutions of higher learning;

- Financial institutions subject, and data collected, processed, or disclosed pursuant to the Gramm-Leach Bliley Act (GLBA); and
- Entities and protected health information covered by the Health Insurance Portability and Accountability Act (HIPPA).

Other data-level exemptions include:

- Data processed by the Fair Credit Reporting Act (FCRA) or by or for a customer reporting agency as defined in the FCRA;
- Data subject to the Driver's Privacy Protection Act; and
- Data covered by the Family Educational Rights and Privacy Act.

What Types of Information Does the Act Cover?

"Personal data" is defined as "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."

"Sensitive data" is defined as "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."

The Act defined the **"sale of personal data"** as "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;
- To a third party for purposes of providing a product or service;
- To an affiliate of the controller;
- Where the customer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party; and
- That the customer:

  (a) intentionally made available to the general public via a channel of mass media; and

  (b) 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.

What Rights Does the Act Create?

"Customer" is defined as "an individual residing in the state action in an individual or household context." As such, the term does not cover individuals acting in a commercial or employment context. Individuals who meet the definition would have the following rights with respect to their personal data:

- Confirm and access;
- Correct inaccuracies;
- Delete; and
- Obtain a copy.

In addition, customers will have the right to opt out of processing their personal data for purposes of targeted advertising, the sale of their personal data, and profiling in furtherance of solely automated decisions.

What Obligations Does the Act Impose?

Controllers will be required to do the following:

1. Provide a privacy policy in its customer agreement or incorporated addendum or in another conspicuous location on its website or online service platform where such notices are customarily posted that:

    (a) Identifies all categories of personal data collected through the website or online service about customers;

    (b) Identifies all third parties to whom the controller has sold or may sell customers personally identifiable information;

    (c) Identifies an active email address or other online mechanism that the customer may use to contact the controller; and

    (d) Clearly and conspicuously discloses that the controller engages in targeted advertising if the controller engages in such advertising.

2. Maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.

3. Conduct data protection impact assessments on the processing of personal data that presents a heightened risk of harm (*g.*, targeted advertising and profiling) after **January 1, 2026**.

4. Do not process "sensitive data" without customer consent, and in the case of a child, in accordance with COPPA.

5. Respond to customer requests within 45 days and provide the information requested for free, once per customer per 12-month period.

6. Do not discriminate against customers who exercise their rights and provide them with the same goods and services at the same price as those customers who do not opt out of the use of their information.

7. Establish binding contracts with processors that:

(a) clearly set forth instructions for processing data;

(b) impose a duty of confidentiality;

(c) require the deletion of personal data at the end of the contract; and

(d) require that the processor cooperate with the controller, including for compliance with the Act's purposes.

How Will the Act Be Enforced?

The Attorney General will have the exclusive authority to enforce the Act and may seek civil penalties of up to $10,000 for each violation, as well as injunctive relief where appropriate. An individual or entity that intentionally discloses personal data may be fined not less than $100 and not more than $500 for each intentional disclosure. There is no private right of action.

Related People

Jason J. Oliveri

Partner

212-471-6237

Related Capabilities

Data Privacy, AI & Cybersecurity

Subscribe to receive timely legal insights directly in your inbox.