2024 -- S 2500

========
LC005228
========

STATE OF RHODE ISLAND

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2024

AN ACT

RELATING TO COMMERCIAL LAW -- GENERAL REGULATORY PROVISIONS -- RHODE ISLAND DATA TRANSPARENCY AND PRIVACY PROTECTION ACT

Introduced By: Senators DiPalma, Euer, and DiMario

Date Introduced: March 01, 2024

Referred To: Senate Commerce

It is enacted by the General Assembly as follows:

SECTION 1. Legislative findings.

The general assembly hereby finds and declares that:

(1) The right to privacy is a personal and fundamental right protected by the United States Constitution. As such, all individuals have a right to privacy in information pertaining to them. This state recognizes the importance of providing customers with transparency about how their personally identifiable information, especially information relating to their children, is shared by businesses. This transparency is crucial for Rhode Island citizens to protect themselves and their families from cyber-crimes and identity thieves.

(2) Furthermore, for free market forces to have a role in shaping the privacy practices and for "opt-in" and "opt-out" remedies to be effective, customers must be more than vaguely informed that a business might share personal data with third parties (as that term is hereinafter defined). Customers must be better informed about what kinds of personally identifiable information is shared with other businesses. With these specifics, customers can knowledgeably choose to opt in, opt out, or choose among businesses that disclose personal data to third parties on the basis of how protective the business is of customers' privacy.

(3) Businesses are now collecting personal data and disclosing it in ways not contemplated or properly covered by the current law. Some websites are installing tracking tools that record when customers visit webpages, and sending personal data, such as age, gender, race, income, health

concerns, religion, and recent purchases to third-party marketers and data brokers. Third-party data broker companies are buying and disclosing personal data obtained from mobile phones, financial institutions, social media sites, and other online and brick and mortar companies. Some mobile applications are sharing personal data, such as location information, unique phone identification numbers, age, gender, and other personal details with third-party companies.

(4) As such, customers need to know the ways that their personal data are being collected by companies and then shared or sold to third parties in order to properly protect their privacy, personal safety, and financial security.

SECTION 2. Title 6 of the General Laws entitled "COMMERCIAL LAW — GENERAL REGULATORY PROVISIONS" is hereby amended by adding thereto the following chapter:

CHAPTER 48.1

RHODE ISLAND DATA TRANSPARENCY AND PRIVACY PROTECTION ACT

6-48.1-1. Short title.

This chapter shall be known and may be cited as the "Rhode Island Data Transparency and Privacy Protection Act".

6-48.1-2. Definitions.

As used in this chapter:

(1) "Affiliate" means any entity that shares common branding with another legal entity directly or indirectly, controls, is controlled by, or is under common control with another legal entity. For this purpose, "control" or "controlled" means ownership of, or the power to vote, more than fifty percent (50%) of the outstanding shares of any class of voting security of a company, control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or the power to exercise controlling influence over the management of a company.

(2) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under this chapter is being made by, or on behalf of, the customer who is entitled to exercise such customer rights with respect to the personal data at issue.

(3) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

(4) "Business associate" has the same meaning as provided in 45 C.F.R. § 160.103.

(5) "Child" has the same meaning as provided in 15 U.S.C. § 6501.

(6) "Consent" means a clear, affirmative act signifying a customer has freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the customer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include acceptance of a general or broad term of use or similar document that contains descriptions of personal data processing along with other, unrelated information, hovering over, muting, pausing or closing a given piece of content, or agreement obtained through the use of dark patterns.

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

(8) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC § 6501 et seq., and the regulations, rules, guidance and exemptions adopted, pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

(9) "Covered entity" has the same meaning as provided in 45 C.F.R. § 160.103.

(10) "Customer" means 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.

(11) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

(12) "Decisions that produce legal or similarly significant effects concerning the customer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

(13) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

(14) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 USC § 1320d et seq., as amended from time to time.

(15) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

(16) "Institution of higher education" means any individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

(17) "Nonprofit organization" means any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding Internal Revenue Code of the United States, as amended from time to time.

(18) "Personal data" means 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.

(19) "Precise geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet (1,750'). "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(20) "Process" or "processing" means 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" means an individual who, or legal entity that, processes personal data on behalf of a controller.

(21) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

(22) "Protected health information" has the same meaning as provided in 42 USC § 1320d.

(23) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information; provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(24) "Publicly available information" means information that is lawfully made available through federal, state or municipal government records or widely distributed media, or a controller has a reasonable basis to believe a customer has lawfully made available to the general public.

(25) "Sale of personal data" means 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, the disclosure of personal data to a third party for purposes of providing a product or service requested by the customer, 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 or intentionally uses the controller to interact with a third party, the disclosure of personal data that the customer:

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

(ii) 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.

(26) "Sensitive data" means 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.

(27) "Targeted advertising" means displaying advertisements to a customer where the advertisement is selected based on personal data obtained or inferred from that customer's activities over time and across nonaffiliated Internet websites or online applications to predict such customer's preferences or interests. "Targeted advertising" does not include advertisements based on activities within a controller's own Internet websites or online applications, advertisements based on the context of a customer's current search query, or current visit to an Internet website or online application, advertisements directed to a customer in response to the customer's request for information or feedback, or processing personal data solely to measure or report advertising frequency, performance or reach.

(28) "Third party" means an individual or legal entity, such as a public authority, agency or body, other than the customer, controller or processor or an affiliate of the processor or of the controller.

(29) "Trade secret" has the same meaning as § 6-41-1.

6-48.1-3. Information sharing practices.

(a) A controller shall, in its customer agreement or incorporated addendum or in another conspicuous location on its website or online service platform where similar notices are customarily posted:

(1) Identify all categories of personal data that the controller collects through the website

or online service about customers;

(2) Identify all categories of third parties to whom the controller may disclose that personally identifiable information;

(3) Identify how customers may exercise their consumer rights, including how a customer may appeal a controller’s decision with regard to the customer’s request;

(4) Identify the purposes for processing the personal data;

(5) Identify the categories of personal data that the controller shares with third parties, if any; and

(6) Identify an active electronic mail address or other online mechanism that the customer may use to contact the controller.

(b) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a customer may exercise the right to opt out of such processing.

(c) Nothing in this chapter shall be construed to authorize the collection, storage or disclosure of information or data that is otherwise prohibited, restricted or regulated by state or federal law.

(d) A controller shall limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which data is processed, as disclosed to the customer. The controller shall not process personal data for purposes that are not reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the customer, unless the controller obtains the customer’s consent.

(e) This chapter does not apply to any body, authority, board, bureau, commission, district or agency of this state or any political subdivision of this state; nonprofit organization; institution of higher education; national securities association that is registered under 15 U.S.C. § 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq.; or covered entity or business associate, as defined in 45 C.F.R. § 160.103.

(f) The following information and data are exempt from the provisions of this chapter:

(1) Protected health information under HIPAA;

(2) Patient-identifying information for purposes of 42 U.S.C. § 290dd-2;

(3) Identifiable private information for purposes of the federal policy for the protection of human research subjects under 45 C.F.R. §§ 46.101 through 46.124;

(4) Identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International

Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;

(5) The protection of human subjects under 21 C.F.R. Parts 50 and 56, or personal data used or shared in research, as defined in 45 C.F.R. § 164.501 or other research conducted in accordance with applicable law;

(6) Information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. § 11101 et seq.;

(7) Patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 U.S.C. § 299b-21 et seq., as amended from time to time;

(8) Information derived from any of the health care related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

(9) Information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 U.S.C. § 290dd-2, as amended from time to time;

(10) Information used for public health activities and purposes as authorized by HIPAA, community health activities and population health activities;

(11) The collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a customer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a customer reporting agency, furnisher or user that provides information for use in a customer report, and by a user of a customer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., as amended from time to time;

(12) Personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq., as amended from time to time;

(13) Personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g et seq., as amended from time to time;

(14) Personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 U.S.C. § 2001 et seq., as amended from time to time;

(15) Data processed or maintained in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or third party, to the extent that the data is collected and used within the context of that role, as the emergency contact information of an individual or that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under this subsection and

used for the purposes of administering such benefits; and

(16) Personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Airline Deregulation Act, 49 U.S.C. § 40101 et seq., as amended from time to time, by an air carrier subject to said act, to the extent subsections 1 to 11, inclusive, of this section are preempted by the Airline Deregulation Act, 49 U.S.C. § 41713, as amended from time to time.

6-48.1-4. Processing of information.

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

(b) The controller shall not process sensitive data concerning a customer without obtaining customer consent and shall not process sensitive data of a child unless consent is obtained and the information is processed in accordance with COPPA.

(c) The controller shall not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against customers.

(d) The controller shall provide the customer with a mechanism to grant and revoke consent where consent is required. Upon receipt of revocation, the controller shall suspend the processing of data as soon as is practicable. The controller shall have no longer than fifteen (15) days from receipt to effectuate the revocation.

6-48.1-5. Customer rights.

(a) No controller shall discriminate against a customer for exercising their customer rights.

(b) No controller shall deny goods or services, charge different prices or rates for goods or services or provide a different level of quality of goods or services to the customer if the customer does not consent to use of their data.

(c) Controllers may provide different prices and levels for goods and services if it is for a bona fide loyalty, rewards, premium features, discount or club card programs that customers voluntarily participate.

(d) A customer shall have the right to:

(1) Confirm whether or not a controller is processing the customer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret;

(2) Correct inaccuracies in the customer's personal data and delete personal data provided by, or obtained about, the customer, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

(3) Obtain a copy of the customer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the customer to transmit the data to another controller without undue delay, where the processing is carried out by automated means; provided such controller shall not be required to reveal any trade secret; and

(4) Opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the customer.

(e) A customer may exercise rights under this section by secure and reliable means established by the controller and described to the customer in the controller's privacy notice. A customer may designate an authorized agent to exercise the rights to opt out on their behalf. In the case of processing personal data of a known child, the parent or legal guardian may exercise such customer rights on the child's behalf. In the case of processing personal data concerning a customer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the customer may exercise such rights on the customer's behalf.

6-48.1-6. Exercising customer rights.

A controller shall comply with a request by a customer to exercise the customer rights authorized as follows:

(1) A controller shall respond to the customer without undue delay, but not later than forty-five (45) days after receipt of the request. The controller may extend the response period by forty-five (45) additional days when reasonably necessary, considering the complexity and number of the customer's requests; provided the controller informs the customer of any such extension within the initial forty-five (45) day response period and of the reason for the extension.

(2) If a controller declines to act regarding the customer's request, the controller shall inform the customer without undue delay, but not later than forty-five (45) days after receipt of the request, of the justification for declining to act and instructions for how to appeal the decision.

(3) Information provided in response to a customer request shall be provided by a controller, free of charge, once per customer during any twelve (12) month period. If requests from a customer are manifestly unfounded, excessive or repetitive, the controller may charge the customer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the customer that the controller is unable to authenticate the

request to exercise such right or rights until such customer provides additional information reasonably necessary to authenticate such customer and such customer's request to exercise such right or rights. A controller shall not be required to authenticate an opt-out request, but may deny an opt-out request if the controller has reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent and that such controller shall not comply with such request.

(5) A controller that has obtained personal data about a customer from a source other than the customer shall be deemed in compliance with a customer's request to delete such data by doing the following:

(i) Retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer’s personal data remains deleted from the controller’s records and not using such retained data for any other purpose pursuant to the provisions of this chapter; or

(ii) Opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of this chapter.

(6) A controller shall establish a process for a customer to appeal the controller's refusal to take action on a request within a reasonable period of time after the customer's receipt of the decision. The appeal process shall be clearly and conspicuously available. Not later than sixty (60) days after receipt of an appeal, a controller shall inform the customer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decision. If the appeal is denied, the customer may submit a complaint to the attorney general.

(7) A customer may designate another person to serve as the customer's authorized agent and act on such customer's behalf, to opt out of the processing of such customer's personal data. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify the identity of the customer and the authorized agent's authority to act on the customer’s behalf.

6-48.1-7. Controller and processor responsibilities.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations of this chapter.

(b) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and 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. The contract shall also require that the processor:

(1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(2) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(3) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations of this chapter;

(4) After providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and

(5) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to assess the processor's policies and technical and organizational measures in support of the obligations of this chapter, using an appropriate and accepted control standard of framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

(c) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under § 6-48.1-8.

(d) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a customer. For the purposes of this section, processing that presents a heightened risk of harm to a customer includes:

(1) The processing of personal data for the purposes of targeted advertising;

(2) The sale of personal data;

(3) The processing of personal data for the purposes of profiling, where such 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 the private affairs or concerns, of customers, where such intrusion would be offensive to a reasonable person, or other substantial injury to customers; and

(4) The processing of sensitive data.

(e) The attorney general may require a controller to disclose any data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller shall make the data protection assessment available. The attorney general may evaluate the data protection assessment for compliance with responsibilities of this chapter. Data protection assessments shall be confidential and shall be exempt from disclosure pursuant to chapter 2 of title 38 ("access to public records"). To the extent any information contained in a data protection assessment disclosed to the attorney general includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

(f) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(g) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(h) Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2025 and are not retroactive.

(i) Any controller in possession of de-identified data shall:

(1) Take reasonable measures to ensure that the data cannot be associated with an individual;

(2) Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

(3) Contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

(j) Nothing in this chapter shall be construed to:

(1) Require a controller or processor to re-identify de-identified data or pseudonymous data; or

(2) Maintain data in identifiable form, or collect, obtain, retain or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(k) Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

(1) Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

(2) Does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with the other personal data about the same specific consumer; and

(3) Does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(l) The rights afforded under this section, and inclusive of § 6-48.1-5(e) shall not apply to pseudonymous data in cases where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

(m) A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

(n) This chapter shall not be construed to restrict a controller's or processor's ability to:

(1) Comply with federal, state or municipal ordinances or regulations;

(2) Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities;

(3) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations;

(4) Investigate, establish, exercise, prepare for or defend legal claims;

(5) Provide a product or service specifically requested by a customer;

(6) Perform under a contract to which a customer is a party, including fulfilling the terms of a written warranty;

(7) Take steps at the request of a customer prior to entering into a contract;

(8) Take immediate steps to protect an interest that is essential for the life or physical safety of the customer or another individual, and where the processing cannot be manifestly based on another legal basis;

(9) Prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action;

(10) Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that

determine, whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller, the expected benefits of the research outweigh the privacy risks, and whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

(11) Assist another controller, processor or third party with any of the obligations of this chapter; or

(12) Process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is:

(i) Subject to suitable and specific measures to safeguard the rights of the customer whose personal data is being processed, and

(ii) Under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(o) The obligations imposed on controllers or processors shall not restrict a controller's or processor's ability to collect, use or retain data for internal use to:

(1) Conduct internal research to develop, improve or repair products, services or technology;

(2) Effectuate a product recall;

(3) Identify and repair technical errors that impair existing or intended functionality; or

(4) Perform internal operations that are reasonably aligned with the expectations of the customer or reasonably anticipated based on the customer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a customer or the performance of a contract to which the customer is a party.

(p) A controller or processor that discloses personal data to a processor or third-party controller shall not be deemed to have violated this chapter if the processor or third-party controller that receives and processes such personal data violates said sections; provided at the time the disclosing controller or processor disclosed such personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller would violate said sections. A third-party controller or processor receiving personal data from a controller or processor in compliance with this chapter is likewise not in violation of said sections for the transgressions of the controller or processor from which such third-party controller or processor receives such personal data.

(q) Nothing in this chapter shall be construed to:

(1) Impose any obligation on a controller or processor that adversely affects the rights or

freedoms of any person, including, but not limited to, the rights of any person to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution; or

(2) Apply to any person's processing of personal data in the course of such person's purely personal or household activities.

(r) Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is reasonably necessary and proportionate to the purposes in this section; and adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used or retained shall, where applicable, consider the nature and purpose or purposes of such collection, use or retention. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to customers relating to such collection, use or retention of personal data.

(s) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption.

(t) Processing personal data for the purposes expressly identified in this section shall not solely make a legal entity a controller with respect to such processing.

6-48.1-8. Violations.

(a) A violation of this chapter constitutes a violation of the general regulatory provisions of commercial law in title 6 and shall constitute a deceptive trade practice in violation of chapter 13.1 of title 6; provided, further, that in the event that 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, for the purposes of circumventing the intent of this chapter;

(2) To any third party that is not exempt pursuant to § 6-48.1-3; or

(3) In violation of any provision of this chapter, that individual or entity shall pay a fine of not less than one hundred dollars ($100) and no more than five hundred dollars ($500) for each such disclosure.

(b) The attorney general shall have sole enforcement authority of the provisions of this chapter and may enforce a violation of this chapter pursuant to:

(1) The provisions of this section; or

(2) General regulatory provisions of commercial law in title 6, or both.

(c) Nothing in this section shall be construed to authorize any private right of action to enforce any provision of this chapter, any regulation hereunder, or any other provisions of law.

6-48.1-9. Waivers - Severability.

Any waiver of the provisions of this chapter shall be void and unenforceable. If any provision of this chapter or its application to any person or circumstance is held invalid by a court of competent jurisdiction, the invalidity shall not affect other provisions of applications of the chapter that can be given effect without the invalid provision or application, and to this end the provisions of the chapter are severable.

6-48.1-10. Construction.

(a) Nothing in this chapter shall be deemed to apply in any manner to a financial institution, an affiliate of a financial institution, or data subject to Title V of the federal Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq. and its implementing regulations, or to information or data subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub. L. 104-191.

(b) Nothing in this chapter shall be construed to apply to a contractor, subcontractor, or agent of a state agency or local unit of government when working for that state agency or local unit of government.

(c) Nothing in this chapter shall be construed to apply to any entity recognized as a tax exempt organization under the Internal Revenue Code.

(d) Nothing in this chapter shall be construed to mandate and/or require the retention or disclosure of any specific individual's personally identifiable information.

(e) Nothing in this chapter shall prohibit or restrict the dissemination or sale of product sales summaries or statistical information or aggregate customer data which may include personally, identifiable information.

(f) Nothing in this chapter shall be construed to apply to any personally identifiable information or any other information collected, used, processed, or disclosed by or for a customer reporting agency as defined by 15 U.S.C. § 1681a(f).

SECTION 3. This act shall take effect on January 1, 2025.

========
LC005228
========

EXPLANATION

BY THE LEGISLATIVE COUNCIL

OF

AN ACT

RELATING TO COMMERCIAL LAW -- GENERAL REGULATORY PROVISIONS --
RHODE ISLAND DATA TRANSPARENCY AND PRIVACY PROTECTION ACT

***

This act would create the Rhode Island Data Transparency and Privacy Protect Act for data privacy protections for the personal data of the citizens of Rhode Island, requiring any person or entity that processes personal data to identify all categories of information the controller collects, when the controller may disclose such information, how a customer may exercise their consumer rights, the purpose for processing the personal data, categories of personal data share with a third party, and means to contact the controller. This act would further limit a controller to processing personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed. A controller would be prohibited from processing sensitive data without obtaining the customer's consent and prohibited from discriminating against a customer for exercising their customer rights. Any violation of this act would constitute a violation of the general regulatory provisions of commercial law and constitute a deceptive trade practice. A fine would be imposed for each violation of not less than one hundred dollars ($100) and no more than five hundred dollars ($500).

This act would take effect on January 1, 2025.

========
LC005228
========