

2024 -- H 7787 SUBSTITUTE A

=====
LC005266/SUB A/2
=====

STATE OF RHODE ISLAND

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2024

A N A C T

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

Introduced By: Representatives Shanley, Batista, Donovan, Edwards, Solomon, Voas,
Dawson, Craven, Vella-Wilkinson, and Handy

Date Introduced: February 29, 2024

Referred To: House Innovation, Internet, & Technology

It is enacted by the General Assembly as follows:

1 SECTION 1. Legislative findings.

2 The general assembly hereby finds and declares that:

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

9 (2) Customers should know whether their personally identifiable information could be sold
10 when they conduct business online or contract with an internet service provider. This information
11 should be readily accessible on the entity's website in a conspicuous location or in a conspicuous
12 location in its customer service agreement. Moreover, entities which control or process data of at
13 least thirty-five thousand (35,000) customers or if they process data of more than ten thousand
14 (10,000) customers and derive more than twenty percent (20%) of their profit from the sale of
15 personally identifiable data should make it possible for customers to opt in and opt out of the
16 collection of their data and control what happens with their personally identifiable information

17 (3) Businesses are now collecting personal data and disclosing it in ways not contemplated
18 or properly covered by the current law. Some websites are installing tracking tools that record when

1 customers visit webpages, and sending personal data, such as age, gender, race, income, health
2 concerns, religion, and recent purchases to third-party marketers and data brokers. Third-party data
3 broker companies are buying and disclosing personal data obtained from mobile phones, financial
4 institutions, social media sites, and other online and brick and mortar companies. Some mobile
5 applications are sharing personal data, such as location information, unique phone identification
6 numbers, age, gender, and other personal details with third-party companies.

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

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

12 CHAPTER 48.1

13 RHODE ISLAND DATA TRANSPARENCY AND PRIVACY PROTECTION ACT

14 **6-48.1-1. Short title.**

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

17 **6-48.1-2. Definitions.**

18 As used in this chapter:

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

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

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

- 1 (4) "Business associate" has the same meaning as provided in 45 C.F.R. § 160.103.
- 2 (5) "Child" has the same meaning as provided in 15 U.S.C. § 6501.
- 3 (6) "Consent" means a clear, affirmative act signifying a customer has freely given,
4 specific, informed and unambiguous agreement to allow the processing of personal data relating to
5 the customer. "Consent" may include a written statement, including by electronic means, or any
6 other unambiguous affirmative action. "Consent" does not include acceptance of a general or broad
7 term of use or similar document that contains descriptions of personal data processing along with
8 other, unrelated information, hovering over, muting, pausing or closing a given piece of content, or
9 agreement obtained through the use of dark patterns.
- 10 (7) "Controller" means an individual who, or legal entity that, alone or jointly with others
11 determines the purpose and means of processing personal data.
- 12 (8) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC § 6501
13 et seq., and the regulations, rules, guidance and exemptions adopted, pursuant to said act, as said
14 act and such regulations, rules, guidance and exemptions may be amended from time to time.
- 15 (9) "Covered entity" has the same meaning as provided in 45 C.F.R. § 160.103.
- 16 (10) "Customer" means an individual residing in this state acting in an individual or
17 household context. "Customer" does not include an individual acting in a commercial or
18 employment context or as an employee, owner, director, officer or contractor of a company,
19 partnership, sole proprietorship, nonprofit or government agency whose communications or
20 transactions with the controller occur solely within the context of that individual's role with the
21 company, partnership, sole proprietorship, nonprofit or government agency.
- 22 (11) "Dark pattern" means a user interface designed or manipulated with the substantial
23 effect of subverting or impairing user autonomy, decision-making or choice, and includes, but is
24 not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".
- 25 (12) "Decisions that produce legal or similarly significant effects concerning the customer"
26 means decisions made by the controller that result in the provision or denial by the controller of
27 financial or lending services, housing, insurance, education enrollment or opportunity, criminal
28 justice, employment opportunities, health care services or access to essential goods or services.
- 29 (13) "De-identified data" means data that cannot reasonably be used to infer information
30 about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such
31 individual.
- 32 (14) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42
33 USC § 1320d et seq., as amended from time to time.
- 34 (15) "Identified or identifiable individual" means an individual who can be readily

1 identified, directly or indirectly.

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

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

9 (18) "Personal data" means any information that is linked or reasonably linkable to an
10 identified or identifiable individual and does not include de-identified data or publicly available
11 information.

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

18 (20) "Process" or "processing" means any operation or set of operations performed,
19 whether by manual or automated means, on personal data or on sets of personal data, such as the
20 collection, use, storage, disclosure, analysis, deletion or modification of personal data. "Processor"
21 means an individual who, or legal entity that, processes personal data on behalf of a controller.

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

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

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

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

34 (25) "Sale of personal data" means the exchange of personal data for monetary or other

1 valuable consideration by the controller to a third party. "Sale of personal data" does not include
2 the disclosure of personal data to a processor that processes the personal data on behalf of the
3 controller, the disclosure of personal data to a third party for purposes of providing a product or
4 service requested by the customer, the disclosure or transfer of personal data to an affiliate of the
5 controller, the disclosure of personal data where the customer directs the controller to disclose the
6 personal data or intentionally uses the controller to interact with a third party, the disclosure of
7 personal data that the customer:

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

9 (ii) Did not restrict to a specific audience, or the disclosure or transfer of personal data to
10 a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a
11 proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes
12 control of all or part of the controller's assets.

13 (26) "Sensitive data" means personal data that includes data revealing racial or ethnic
14 origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation
15 or citizenship or immigration status, the processing of genetic or biometric data for the purpose of
16 uniquely identifying an individual, personal data collected from a known child, or precise
17 geolocation data.

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

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

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

31 **6-48.1-3. Information sharing practices.**

32 (a) Any commercial website or internet service provider conducting business in Rhode
33 Island or with customers in Rhode Island or otherwise subject to Rhode Island jurisdiction, shall
34 designate a controller. If a commercial website or Internet service provider collects, stores and sells

1 customers' personally identifiable information, then the controller shall, in its customer agreement
2 or incorporated addendum, or in another conspicuous location on its website or online service
3 platform where similar notices are customarily posted:

4 (1) Identify all categories of personal data that the controller collects through the website
5 or online service about customers;

6 (2) Identify all third parties to whom the controller has sold or may sell customers'
7 personally identifiable information; and

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

10 (b) If a controller sells personal data to third parties or processes personal data for targeted
11 advertising, the controller shall clearly and conspicuously disclose such processing.

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

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

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

21 (1) Protected health information under HIPAA;

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

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

25 (4) Identifiable private information that is otherwise information collected as part of human
26 subjects research pursuant to the good clinical practice guidelines issued by the International
27 Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;

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

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

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

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

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

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

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

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

18 (13) Personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C.
19 § 1232g et seq., as amended from time to time;

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

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

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

33 **6-48.1-4. Processing of information.**

34 (a) This section shall apply to for-profit entities that conduct business in the state or for-

1 profit entities that produce products or services that are targeted to residents of the state and that
2 during the preceding calendar year did any of the following:

3 (1) Controlled or processed the personal data of not less than thirty-five thousand (35,000)
4 customers, excluding personal data controlled or processed solely for the purpose of completing a
5 payment transaction.

6 (2) Controlled or processed the personal data of not less than ten thousand (10,000)
7 customers and derived more than twenty percent (20%) of their gross revenue from the sale of
8 personal data.

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

12 (c) The controller shall not process sensitive data concerning a customer without obtaining
13 customer consent and shall not process sensitive data of a known child unless consent is obtained
14 and the information is processed in accordance with COPPA. Controllers and processors that
15 comply with the verifiable parental consent requirements of the Children's Online Privacy
16 Protection Act (15 U.S.C. § 6501 et seq.) shall be deemed compliant with any obligation to obtain
17 parental consent under this chapter.

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

20 (e) The controller shall provide customers with a mechanism to grant and revoke consent
21 to collect, store and sell their personally identifiable information. Upon receipt of revocation, the
22 controller shall suspend the processing of data as soon as is practicable. The controller shall have
23 no longer than fifteen (15) days from receipt to effectuate the revocation.

24 **6-48.1-5. Customer rights.**

25 (a) This section shall apply to for-profit entities that conduct business in the state or for-
26 profit entities that produce products or services that are targeted to residents of the state and that
27 during the preceding calendar year did any of the following:

28 (1) Controlled or processed the personal data of not less than thirty-five thousand (35,000)
29 customers, excluding personal data controlled or processed solely for the purpose of completing a
30 payment transaction.

31 (2) Controlled or processed the personal data of not less than ten thousand (10,000)
32 customers and derived more than twenty percent (20%) of their gross revenue from the sale of
33 personal data.

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

1 (c) No controller shall deny goods or services, charge different prices or rates for goods or
2 services or provide a different level of quality of goods or services to the customer if the customer
3 does not consent to use of their data. However, if a customer opts out of data collection, the covered
4 entity is not required to provide a service that requires this data collection.

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

8 (e) A customer shall have the right to:

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

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

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

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

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

29 **6-48.1-6. Exercising customer rights.**

30 (a) This section shall apply to for-profit entities that conduct business in the state or for-
31 profit entities that produce products or services that are targeted to residents of the state and that
32 during the preceding calendar year did any of the following:

33 (1) Controlled or processed the personal data of not less than thirty-five thousand (35,000)
34 customers, excluding personal data controlled or processed solely for the purpose of completing a

1 payment transaction.

2 (2) Controlled or processed the personal data of not less than ten thousand (10,000)
3 customers and derived more than twenty percent (20%) of their gross revenue from the sale of
4 personal data.

5 (b) A controller shall comply with a request by a customer to exercise the customer rights
6 authorized as follows:

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

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

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

21 (4) If a controller is unable to authenticate a request to exercise any of the rights afforded,
22 the controller shall not be required to comply with a request to initiate an action pursuant to this
23 section and shall provide notice to the customer that the controller is unable to authenticate the
24 request to exercise such right or rights until such customer provides additional information
25 reasonably necessary to authenticate such customer and such customer's request to exercise such
26 right or rights. A controller shall not be required to authenticate an opt-out request, but may deny
27 an opt-out request if the controller has reasonable and documented belief that such request is
28 fraudulent. If a controller denies an opt-out request because the controller believes such request is
29 fraudulent, the controller shall send a notice to the person who made such request disclosing that
30 such controller believes such request is fraudulent, why such controller believes such request is
31 fraudulent and that such controller shall not comply with such request.

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

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

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

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

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

17 **6-48.1-7. Controller and processor responsibilities.**

18 (a) This section shall apply to for-profit entities that conduct business in the state or for-
19 profit entities that produce products or services that are targeted to residents of the state and that
20 during the preceding calendar year did any of the following:

21 (1) Controlled or processed the personal data of not less than thirty-five thousand (35,000)
22 customers, excluding personal data controlled or processed solely for the purpose of completing a
23 payment transaction.

24 (2) Controlled or processed the personal data of not less than ten thousand (10,000)
25 customers and derived more than twenty percent (20%) of their gross revenue from the sale of
26 personal data.

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

29 (c) A contract between a controller and a processor shall govern the processor's data
30 processing procedures with respect to processing performed on behalf of the controller. The
31 contract shall be binding and clearly set forth instructions for processing data, the nature and
32 purpose of processing, the type of data subject to processing, the duration of processing and the
33 rights and obligations of both parties. The contract shall also require that the processor:

34 (1) Ensure that each person processing personal data is subject to a duty of confidentiality

1 with respect to the data:

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

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

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

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

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

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

25 (1) The processing of personal data for the purposes of targeted advertising;
26 (2) The sale of personal data;
27 (3) The processing of personal data for the purposes of profiling, where such profiling
28 presents a reasonably foreseeable risk of unfair or deceptive treatment of, or unlawful disparate
29 impact on, customers, financial, physical or reputational injury to customers, a physical or other
30 intrusion upon the solitude or seclusion, or the private affairs or concerns, of customers, where such
31 intrusion would be offensive to a reasonable person, or other substantial injury to customers; and
32 (4) The processing of sensitive data.

33 (f) The attorney general may require a controller to disclose any data protection assessment
34 that is relevant to an investigation conducted by the attorney general, and the controller shall make

1 the data protection assessment available. The attorney general may evaluate the data protection
2 assessment for compliance with responsibilities of this chapter. Data protection assessments shall
3 be confidential and shall be exempt from disclosure pursuant to chapter 2 of title 38 ("access to
4 public records"). To the extent any information contained in a data protection assessment disclosed
5 to the attorney general includes information subject to attorney-client privilege or work product
6 protection, such disclosure shall not constitute a waiver of such privilege or protection.

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

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

14 (i) Data protection assessment requirements shall apply to processing activities created or
15 generated after January 1, 2026 and are not retroactive.

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

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

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

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

23 (k) Nothing in this chapter shall be construed to:

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

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

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

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

33 (2) Does not use the personal data to recognize or respond to the specific customer who is
34 the subject of the personal data, or associate the personal data with the other personal data about

1 the same specific customer; and

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

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

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

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

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

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

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

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

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

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

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

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

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

30 (10) Engage in public or peer-reviewed scientific or statistical research in the public interest
31 that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed
32 by an institutional review board that determines, or similar independent oversight entities that
33 determine, whether the deletion of the information is likely to provide substantial benefits that do
34 not exclusively accrue to the controller, the expected benefits of the research outweigh the privacy

1 risks, and whether the controller has implemented reasonable safeguards to mitigate privacy risks
2 associated with research, including any risks associated with re-identification;

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

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

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

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

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

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

15 (2) Effectuate a product recall;

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

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

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

31 (r) Nothing in this chapter shall be construed to:

32 (1) Impose any obligation on a controller or processor that adversely affects the rights or
33 freedoms of any person, including, but not limited to, the rights of any person to freedom of speech
34 or freedom of the press guaranteed in the First Amendment to the United States Constitution; or

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

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

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

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

15 (v) If a customer opts out of data collection, the covered entity is not required to provide a
16 service that requires this data collection.

17 **6-48.1-8. Violations.**

18 (a) A violation of this chapter constitutes a violation of the general regulatory provisions
19 of commercial law in title 6 and shall constitute a deceptive trade practice in violation of chapter
20 13.1 of title 6; provided, further, that in the event that any individual or entity intentionally discloses
21 personal data:

22 (1) To a shell company or any entity that has been formed or established solely, or in part,
23 for the purposes of circumventing the intent of this chapter; or

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

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

29 (1) The provisions of this section; or

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

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

33 **6-48.1-9. Waivers - Severability.**

34 Any waiver of the provisions of this chapter shall be void and unenforceable. If any

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

5 **6-48.1-10. Construction.**

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

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

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

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

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

20 (f) Nothing in this chapter shall be construed to apply to any personally identifiable
21 information or any other information collected, used, processed, or disclosed by or for a customer
22 reporting agency as defined by 15 U.S.C. § 1681a(f). Provided, further, nothing in this chapter shall
23 be construed to require any entity to collect, store or sell personally identifiable information, and
24 furthermore, nothing in this chapter shall be construed to require a controller to provide a good or
25 service that requires the personal data of a customer that the controller does not collect or maintain.
26 This chapter is intended to apply only to covered entities that choose to collect, store, and sell or
27 otherwise transfer or disclose personally identifiable information. The obligations imposed on
28 controllers or processors under this chapter shall not apply where compliance by the controller or
29 processor with this chapter would violate an evidentiary privilege under the law of this state.
30 Nothing in this chapter shall be construed to prevent a controller or processor from providing
31 personal data concerning a customer to a person covered by an evidentiary privilege under the laws
32 of this state as part of a privileged communication.

1 SECTION 3. This act shall take effect on January 1, 2026.

=====
LC005266/SUB A/2
=====

EXPLANATION
BY THE LEGISLATIVE COUNCIL
OF

A N A C T

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

1 This act would create the Rhode Island Data Transparency and Privacy Protect Act for data
2 privacy protections for the personal data of the citizens of Rhode Island, requiring any person or
3 entity that processes personal data to identify all categories of information the controller collects,
4 when the controller may disclose such information, how a customer may exercise their customer
5 rights, the purpose for processing the personal data, categories of personal data share with a third
6 party, and means to contact the controller. Entities that control or process personal data of not less
7 than 35,000 customers or at least 10,000 customers and derive more than twenty percent (20%) of
8 gross revenue from the sale of personal data are subject to additional disclosure requirements and
9 must allow customers the right to opt out of the collection of personally identifiable information.
10 Any violation of this act would constitute a violation of the general regulatory provisions of
11 commercial law and constitute a deceptive trade practice. A fine would be imposed for each
12 violation of not less than one hundred dollars (\$100) and no more than five hundred dollars (\$500).

13 This act would take effect on January 1, 2026.

=====
LC005266/SUB A/2
=====