

LC005126

JANUARY SESSION, A.D. 2026

RELATING TO COMMERCIAL LAW -- GENERAL REGULATORY PROVISIONS -- AGE-
APPROPRIATE DESIGN CODE

Referred To: House Innovation, Internet, & Technology

(4) "Collect" means buying, renting, gathering, obtaining, receiving, or accessing any personal data pertaining to a consumer by any means, including receiving data from the consumer.

1 either actively or passively, or by observing the consumer's behavior.

2 (5) "Common branding" means a shared name, service mark, or trademark that the average
3 consumer would understand that two (2) or more entities are commonly owned. For purposes of
4 this chapter, for a joint venture or partnership composed of covered entities in which each covered
5 entity has at least a forty percent (40%) interest, the joint venture or partnership and each covered
6 entity that composes the joint venture or partnership shall separately be considered a single covered
7 entity, except that personal data in the possession of each covered entity and disclosed to the joint
8 venture or partnership shall not be shared with the other covered entity.

9 (6) "Consumer" means a natural person who is a Rhode Island resident, however identified,
10 including by any unique identifier.

11 (7) "Covered entity" means:

12 (i) A sole proprietorship, partnership, limited liability company, corporation, association,
13 or other legal entity that is organized or operated for the profit or financial benefit of its shareholders
14 or other owners engaged in an activity pursuant to the provisions of § 6-48.2-2;

15 (ii) An affiliate of a covered entity that shares common branding with the covered entity.

16 (8) "Dark pattern" means a user interface designed or manipulated with the purpose of
17 subverting or impairing user autonomy, decision making, or choice.

18 (9) "Default" means a preselected option adopted by the covered entity for the online
19 service, product, or feature.

20 (10) "Deidentified" means data that cannot reasonably be used to infer information about,
21 or otherwise be linked to, an identified or identifiable consumer, or a device linked to such
22 consumer; provided that, the covered entity that possesses the data:

23 (i) Takes reasonable measures to ensure that the data cannot be associated with a consumer;
24 (ii) Publicly commits to maintain and use the data only in a deidentified fashion and not
25 attempt to re-identify the data; and

26 (iii) Contractually obligates any recipients of the data to comply with all provisions of this
27 chapter.

28 (11) "Derived data" means data that is created by the derivation of information, data,
29 assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or another
30 source of information or data about a known child or a child's device.

31 (12) "Online service, product, or feature" means access to various types of data on the
32 Internet, including banking, education, entertainment, news, shopping and commercial services.
33 "Online service, product, or feature" does not mean any of the following:

34 (i) "Telecommunications service," as defined in 47 U.S.C. § 153;

1 (ii) A broadband Internet access service; or

2 (iii) The sale, delivery, or use of a physical product.

3 (13) "Personal data" means any information, including derived data, that is linked or
4 reasonably linkable, alone or in combination with other information, to an identified or identifiable
5 consumer. Personal data does not include deidentified data or publicly available information.

6 (14) "Precise geolocation" means any data that is derived from a device and that is used or
7 intended to be used to locate a consumer within a geographic area that is equal to or less than the
8 area of a circle with a radius of one thousand eight hundred fifty feet (1,850').

9 (15) "Process" or "processing" means to conduct or direct any operation or set of operations
10 performed, whether by manual or automated means, on personal data or on sets of personal data,
11 such as the collection, use, storage, disclosure, analysis, deletion, modification, or otherwise
12 handling of personal data.

13 (16) "Product experimentation results" means the data that companies collect to understand
14 the experimental impact of their products.

15 (17) "Profile" or "profiling" means any form of automated processing of personal data to
16 evaluate, analyze, or predict personal aspects concerning an identified or identifiable consumer's
17 economic situation, health, personal preferences, interests, reliability, behavior, location, or
18 movements. "Profiling" does not include the processing of information that does not result in an
19 assessment or judgment about a consumer.

20 (18) "Publicly available information" means information that either:

21 (i) Is made available from federal, state, or local government records or widely distributed
22 media; or

23 (ii) A covered entity has a reasonable basis to believe a consumer has lawfully made
24 available to the public such that the consumer no longer has a reasonable expectation of privacy in
25 the information.

26 (19) "Sale," "sell," or "sold" means the exchange of personal data for monetary or other
27 valuable consideration by a covered entity to a third party. It does not include the following:

28 (i) The disclosure of personal data to a third party who processes the personal data on behalf
29 of the covered entity;

30 (ii) The disclosure of personal data to a third party with whom the consumer has a direct
31 relationship for purposes of providing a product or service requested by the consumer;

32 (iii) The disclosure or transfer of personal data to an affiliate of the covered entity;

33 (iv) The disclosure of data that the consumer intentionally made available to the general
34 public such that the consumer no longer maintains a reasonable expectation of privacy in the data;

1 or

2 (v) The disclosure or transfer of personal data to a third party as an asset that is part of a
3 completed or proposed merger, acquisition, bankruptcy, or other transaction in which the third party
4 assumes control of all or part of the covered entity's assets, provided the consumer has the
5 opportunity to opt out of the transfer.

6 (20) "Share" means sharing, renting, releasing, disclosing, disseminating, making
7 available, transferring, or otherwise communicating orally, in writing, or by electronic or other
8 means a consumer's personal data by the covered entity to a third party for cross-context behavioral
9 advertising, whether or not for monetary or other valuable consideration, including transactions
10 between a covered entity and a third party for cross-context behavioral advertising for the benefit
11 of a covered entity in which no money is exchanged.

12 (21) "Third party" means a natural or legal person, public authority, agency, or body, other
13 than the consumer or the covered entity.

14 **6-48.2-2. Scope - Exclusions.**

15 (a) An entity is considered a covered entity for the purposes of this chapter if the entity:

16 (1) Collects consumers' personal data or has individuals' personal data collected on the
17 entity's behalf by a third party;

18 (2) Alone or jointly with others, determines the purposes and means of the processing of
19 individuals' personal data;

20 (3) Operates in Rhode Island; and

21 (4) Satisfies one or more of the following thresholds:

22 (i) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as
23 adjusted every odd-numbered year to reflect any changes in the Consumer Price Index;

24 (ii) Alone or in combination, annually buys, receives for the covered entity's commercial
25 purposes, sells, or shares for commercial purposes, alone or in combination, the personal data of
26 fifty thousand (50,000) or more individuals, households, or devices; or

27 (iii) Derives fifty percent (50%) or more of its annual revenues from selling individuals'
28 personal data.

29 (b) This chapter shall not apply to:

30 (1) Protected health information that is collected by a covered entity or covered entity
31 associate governed by the privacy, security, and breach notification rules issued by the U.S.
32 Department of Health and Human Services (45 CFR Parts 160 and 164);

33 (2) A covered entity governed by the privacy, security, and breach notification rules issued
34 by the U.S. Department of Health and Human Services (45 CFR Parts 160 and 164) to the extent

1 the provider or covered entity maintains patient information in the same manner as medical
2 information or protected health information as described in subsection (b)(1) of this section; and

3 (3) Information collected as part of a clinical trial subject to the federal Policy for the
4 Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice
5 guidelines issued by the International Council for Harmonisation of Technical Requirements for
6 Pharmaceuticals for Human Use or pursuant to human subject protection requirements of the U.S.
7 Food and Drug Administration.

8 (c) Nothing in this chapter shall be interpreted to interfere with any obligation or
9 requirement under chapter 48.1 of title 6. The covered entity authorized pursuant to § 6-48.1-4
10 regarding sensitive data concerning known children shall have no additional obligation pursuant to
11 this chapter.

12 **6-48.2-3. Heightened risk of harm to children -- Presumption -- Definitions.**

13 (a) Each covered entity that offers any online service, product or feature to a consumer
14 whom such covered entity has actual knowledge, or willfully disregards is a child shall use
15 reasonable care to avoid any heightened risk of harm to children caused by such online service,
16 product or feature. In any enforcement action brought by the attorney general pursuant to § 6-48.2-
17 7, there shall be a rebuttable presumption that a covered entity used reasonable care as required
18 under this section if the covered entity complied with the provisions of § 6-48.2-4 concerning data
19 protection assessments.

20 (b) As used in this chapter, “heightened risk of harm to children” means processing known
21 children’s personal data in a manner that presents any reasonably foreseeable risk of:

22 (1) Any unfair or deceptive treatment of, or any unlawful disparate impact on, children;

23 (2) Any financial or reputational injury to children;

24 (3) Any physical or other intrusion upon the solitude or seclusion, or the private affairs or
25 concerns, of children if such intrusion would be highly offensive to a reasonable person; or

26 (4) Discrimination against the child based upon race, color, religion, national origin,
27 disability, sex, sexual orientation, or gender identity or expression.

28 **6-48.2-4. Covered entity obligations.**

29 (a) A covered entity subject to this chapter shall:

30 (1) Complete a data protection impact assessment for an online service, product, or feature
31 that is reasonably likely to be accessed by children and maintain documentation of the data
32 protection impact assessment for as long as the online service, product, or feature is reasonably
33 known to be used by children. The data protection impact assessment shall consist of a systematic
34 survey to assess compliance with the duty to use reasonable care to avoid any heightened risk of

1 harm to known children and shall include a plan to ensure that all online products, services, or
2 features provided by the covered entity and known to be used by children are designed and offered
3 in a manner consistent with the duty to use reasonable care to avoid any heightened risk of harm to
4 known children. The plan shall include a description of steps the covered entity has taken and shall
5 take to comply with the duty to use reasonable care to avoid any heightened risk of harm to known
6 children.

7 (2) Review and modify all data protection impact assessments as necessary to account for
8 material changes to processing pertaining to the online service, product, or feature within ninety
9 (90) days after any material changes.

10 (3) Within five (5) days after receipt of a written request by the attorney general, provide
11 to the attorney general a list of all data protection impact assessments the covered entity has
12 completed.

13 (4) Within seven (7) days after receipt of a written request by the attorney general, provide
14 the attorney general with a copy of a data protection impact assessment; provided that, the attorney
15 general may, in the attorney general's discretion, extend beyond seven (7) days the amount of time
16 allowed for a covered entity to produce a data protection impact assessment.

17 (5) Configure all default privacy settings provided to known children by the online service,
18 product, or feature to settings that offer a high level of privacy, unless the covered entity can
19 demonstrate a compelling reason that a different setting is consistent with the duty to use reasonable
20 care to avoid any heightened risk of harm to children, as defined pursuant to the provisions of § 6-
21 48.2-3(b).

22 (6) Provide any privacy information, terms of service, policies, and community standards
23 concisely, prominently, and using clear language suited to the age of children known to access that
24 online service, product, or feature.

25 (7) Provide prominent, accessible, and responsive tools to assist known children in a form
26 or manner required by the attorney general, or, if applicable, their parents or guardians, in the
27 exercise of their privacy rights and to report concerns.

28 (b) A data protection impact assessment required by this section shall:

29 (1) Identify the purpose of the online service, product, or feature;

30 (2) Disclose how it uses children's personal data; and

31 (3) Determine whether the online service, product, or feature is designed and offered in a
32 manner consistent with the duty to use reasonable care to avoid any heightened risk of harm to
33 children and;

34 (i) Whether the design of the online service, product, or feature is reasonably expected to

1 allow known children to be party to or exploited by a contract on the online service, product, or
2 feature that would result in reasonably foreseeable and material financial harm to the child; a highly
3 offensive intrusion on the reasonable privacy expectations of the child; or discrimination against
4 the child based upon race, color, religion, national origin, disability, sex, sexual orientation, or
5 gender identity or expression;

6 (ii) Whether targeted advertising systems used by the online service, product, or feature
7 would result in reasonably foreseeable and material financial harm to the known child; a highly
8 offensive intrusion on the reasonable privacy expectations of the child; or discrimination against
9 the child based upon race, color, religion, national origin, disability, sex, sexual orientation, or
10 gender identity or expression;

11 (iii) Whether the online service, product, or feature uses system design features to increase,
12 sustain, or extend use of the online service, product, or feature by known children, including the
13 automatic playing of media, rewards for time spent, and notifications, that would result in
14 reasonably foreseeable and material financial harm to the child or a highly offensive intrusion on
15 the reasonable privacy expectations of the child; or discrimination against the child based upon
16 race, color, religion, national origin, disability, sex, sexual orientation, or gender identity or
17 expression;

18 (iv) Whether, how, and for what purpose the online product, service, or feature collects or
19 processes personal data of known children and whether those practices would result in reasonably
20 foreseeable and material financial harm to the child; a highly offensive intrusion on the reasonable
21 privacy expectations of the child; or discrimination against the child based upon race, color,
22 religion, national origin, disability, sex, sexual orientation, or gender identity or expression; and

23 (v) Whether and how product experimentation results for the online product, service, or
24 feature reveal data management or design practices that would result in reasonably foreseeable and
25 material financial harm to the known child; a highly offensive intrusion on the reasonable privacy
26 expectations of the child; or discrimination against the child based upon race, color, religion,
27 national origin, disability, sex, sexual orientation, or gender identity or expression.

28 (c) A data protection impact assessment conducted by a covered entity for the purpose of
29 compliance with any other law may be utilized to comply with the provisions of this chapter if the
30 data protection impact assessment meets the requirements of this chapter.

31 (d) A single data protection impact assessment may contain multiple similar processing
32 operations that present similar risk only if each relevant online service, product, or feature is
33 addressed separately.

34 (e) A covered entity may process only the personal data reasonably necessary to provide

1 an online service, product, or feature with which a child is actively and knowingly engaged to
2 estimate age.

3 (f) A data protection impact assessment created pursuant to this section is exempt from
4 public disclosure and to the extent required to be disclosed to public officials shall not constitute a
5 public record pursuant to the provisions of chapter 2 of title 38 (“access to public records”).

6 **6-48.2-5. Covered entity prohibitions.**

7 A covered entity that provides an online service, product, or feature to known children shall
8 not:

9 (1) Process the personal data of any known child in a way that is inconsistent with the duty
10 to use reasonable care to avoid any heightened risk of harm to children, as defined pursuant to the
11 provisions of § 6-48.2-3(b);

12 (2) Profile a known child by default unless both of the following criteria are met:

13 (i) The covered entity can demonstrate it has appropriate safeguards in place to ensure that
14 profiling is consistent with the duty to use reasonable care to avoid any heightened risk of harm to
15 known children; and

16 (ii) Profiling is necessary to provide the online service, product, or feature requested and
17 only with respect to the aspects of the online service, product, or feature with which a known child
18 is actively and knowingly engaged;

19 (3) Process any personal data that is not reasonably necessary to provide an online service,
20 product, or feature with which a known child is actively and knowingly engaged;

21 (4) If the end user is a known child, process personal data for any reason other than a reason
22 for which that personal data was collected;

23 (5) Process any precise geolocation information of known children by default, unless the
24 collection of that precise geolocation information is strictly necessary for the covered entity to
25 provide the service, product, or feature requested and then only for the limited time that the
26 collection of precise geolocation information is necessary to provide the service, product, or
27 feature;

28 (6) Process any precise geolocation information of a known child without providing a
29 conspicuous sign to the child for the duration of that collection that precise geolocation information
30 is being collected;

31 (7) Use dark patterns to cause known children to provide personal data beyond what is
32 reasonably expected to provide that online service, product, or feature to forego privacy protections,
33 or to take any action that the covered entity knows, or has reason to know, is not consistent with
34 the duty to use reasonable care to avoid any heightened risk of harm to children; or

1 (8) Allow a known child's parent or any other consumer to monitor the child's online
2 activity or track the child's location, without providing a conspicuous signal to the child when the
3 child is being monitored or tracked.

4 **6-48.2-6. Impact assessments non-public information.**

5 (a) A data protection impact assessment collected or maintained by the attorney general
6 pursuant to this chapter shall not be deemed public for purposes of chapter 2 of title 38 ("access to
7 public records").

8 (b) To the extent any information contained in a data protection impact assessment
9 disclosed to the attorney general includes information subject to attorney-client privilege or work
10 product protection, disclosure pursuant to this chapter does not constitute a waiver of that privilege
11 or protection.

12 **6-48.2-7. Enforcement.**

13 (a) The attorney general may seek the imposition of an injunction and a civil penalty of not
14 more than two thousand five hundred dollars (\$2,500) per affected child for each negligent violation
15 of this chapter, or not more than seven thousand five hundred dollars (\$7,500) per affected child
16 for each intentional violation of this chapter, plus costs and reasonable attorneys' fees for each
17 violation.

18 (b) Any penalties, fees, and expenses recovered in an action brought under this chapter
19 shall be deposited in a restricted receipt account and are to be appropriated to the attorney general
20 and utilized pursuant to the provisions of subsection (c) of this section.

21 (c) All fees collected by the office of the attorney general in accordance with subsection
22 (b) of this section shall be placed into a restricted receipt account to support the personnel costs,
23 operating costs and capital expenditure necessary to carry out the enforcement provisions of this
24 section; provided, however, that any fees charged shall be in addition to and not substituted for
25 funds appropriated for the office by the state or federal government.

26 (d) If a covered entity is in substantial compliance with the requirements of this chapter,
27 the attorney general shall, before initiating a civil action pursuant to the provisions of this chapter,
28 provide written notice to the covered entity identifying the specific provisions of this chapter that
29 the attorney general alleges have been or are being violated. If a covered entity satisfies the
30 provisions of § 6-48.2-4 before offering any new online product, service, or feature reasonably
31 likely to be accessed by children to the public, the covered entity shall have ninety (90) days to
32 fully comply with all provisions specified in the notice from the attorney general. If the covered
33 entity cures all noticed violations and provides the attorney general a written statement that the
34 alleged violations have been cured, and sufficient measures have been taken to prevent future

1 violations, the covered entity shall not be liable for a civil penalty for any violation cured within
2 the ninety (90) day period.

3 (e) No individual entitlement or private right of action is created by this section.

4 SECTION 2. This act shall take effect on January 1, 2027.

=====
LC005126
=====

EXPLANATION
BY THE LEGISLATIVE COUNCIL
OF
A N A C T
RELATING TO COMMERCIAL LAW -- GENERAL REGULATORY PROVISIONS -- AGE-
APPROPRIATE DESIGN CODE

- 1 This act would require that any covered entity that develops and provides online services,
2 products, or features that children are reasonably likely to access shall consider the best interest of
3 children when designing and developing such online service, product, or feature. The provisions of
4 this chapter may be enforced by the attorney general and violators are subject to civil penalties.
5 This act would take effect on January 1, 2027.

=====
LC005126
=====