
A BILL FOR AN ACT

RELATING TO CONSUMER DATA PROTECTION.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

1 SECTION 1. The Hawaii Revised Statutes is amended by
2 adding a new chapter to title 26 to be appropriately designated
3 and to read as follows:

4 "CHAPTER

5 CONSUMER DATA PROTECTION ACT

6 § -1 Definitions. As used in this chapter, unless the
7 context otherwise requires:

8 "Affiliate" means a legal entity that controls, is
9 controlled by, or is under common control with another legal
10 entity or shares common branding with another legal entity.

11 Solely for the purposes of this definition, "control" or
12 "controlled" means:

13 (1) Ownership of, or the power to vote, more than fifty
14 per cent of the outstanding shares of any class of
15 voting security of a company;



1 (2) Control in any manner over the election of a majority
2 of the directors or of individuals exercising similar
3 functions; or

4 (3) Power to exercise controlling influence over the
5 management of a company.

6 "Authenticate" means to verify through reasonable means
7 that a consumer attempting to exercise the consumer rights
8 specified in section -3 is the actual consumer with the
9 consumer rights with respect to the personal data at issue.

10 "Biometric data" means data generated by automatic
11 measurements of an individual's biological characteristics,
12 including fingerprints, voiceprints, eye retinas, irises, or
13 other unique biological patterns or characteristics that are
14 used to identify a specific individual. The term "biometric
15 data" does not include a physical or digital photograph, a video
16 or audio recording or data generated therefrom, or information
17 collected, used, or stored for health care treatment, payment,
18 or operations under the Health Insurance Portability and
19 Accountability Act.



1 "Business associate" shall have the same meaning as the
2 term is defined in title 45 Code of Federal Regulations section
3 160.103.

4 "Child" means any natural person younger than thirteen
5 years of age.

6 "Consent" means a written statement, including a statement
7 written by electronic means, or any other unambiguous and clear
8 affirmative act signifying a consumer's freely-given, specific,
9 informed, and unambiguous agreement to process personal data
10 relating to the consumer.

11 "Consumer" means a natural person who is a resident of the
12 State acting only in an individual or household context. The
13 term "consumer" does not include a natural person acting in a
14 commercial or employment context.

15 "Controller" means the natural or legal person that, alone
16 or jointly with others, determines the purpose and means of
17 processing personal data.

18 "Covered entity" shall have the same meaning as the term is
19 defined in title 45 Code of Federal Regulations section 160.103.



1 "De-identified data" means data that cannot reasonably be
2 linked to an identified or identifiable natural person, or a
3 device linked to the person.

4 "Department" means the department of the attorney general.

5 "Health Insurance Portability and Accountability Act" means
6 the Health Insurance Portability and Accountability Act of 1996,
7 P.L. 104-191, as amended.

8 "Identified or identifiable natural person" means a natural
9 person who can be readily identified, directly, or indirectly.

10 "Institution of higher education" means:

- 11 (1) The University of Hawaii system, or one of its
12 campuses; or
- 13 (2) A private college or university authorized to operate
14 in the State pursuant to chapter 305J.

15 "Nonprofit organization" means any:

- 16 (1) Corporation incorporated pursuant to chapter 414D;
- 17 (2) Organization exempt from taxation under section
18 501(c)(3), (6), or (12) of the Internal Revenue Code
19 of 1986, as amended; or
- 20 (3) Consumer cooperative association subject to chapter
21 421C.



1 "Personal data" means any information that is linked or
2 could be reasonably linkable to an identified or identifiable
3 natural person. The term "personal data" does not include de-
4 identified data or publicly available information.

5 "Precise geolocation data" means information derived from
6 technology, including global positioning system level latitude
7 and longitude coordinates or other mechanisms, that directly
8 identifies the specific location of a natural person with
9 precision and accuracy within a radius of 1,750 feet. The term
10 "precise geolocation data" does not include the content of
11 communications or any data generated by or connected to advanced
12 utility metering infrastructure systems or equipment for use by
13 a utility.

14 "Process" or "processing" means any operation or set of
15 operations performed, whether by manual or automated means, on
16 personal data or on sets of personal data, including the
17 collection, use, storage, disclosure, analysis, deletion, or
18 modification of personal data.

19 "Processor" means a natural or legal person that processes
20 personal data on behalf of a controller.



1 "Profiling" means any form of automated processing
2 performed on personal data to evaluate, analyze, or predict
3 personal aspects related to an identified or identifiable
4 natural person's economic situation, health, personal
5 preferences, interests, reliability, behavior, location, or
6 movements.

7 "Pseudonymous data" means personal data that cannot be
8 attributed to a specific natural person without the use of
9 additional information.

10 "Publicly available information" means information that is
11 lawfully made available through federal, state, or local
12 government records, or information that a business has a
13 reasonable basis to believe is lawfully made available to the
14 general public through widely distributed media, by the
15 consumer, or by a person to whom the consumer has disclosed the
16 information, unless the consumer has restricted the
17 information to a specific audience.

18 "Sale of personal data" means the exchange of personal data
19 for monetary consideration by the controller to a third party.

20 The term "sale of personal data" does not include:



- 1 (1) The disclosure of personal data to a processor that
- 2 processes the personal data on behalf of the
- 3 controller;
- 4 (2) The disclosure of personal data to a third party for
- 5 purposes of providing a product or service requested
- 6 by the consumer;
- 7 (3) The disclosure or transfer of personal data to an
- 8 affiliate of the controller;
- 9 (4) The disclosure of information that the consumer:
- 10 (A) Intentionally made available to the general
- 11 public via a channel of mass media; and
- 12 (B) Did not restrict to a specific audience; or
- 13 (5) The disclosure or transfer of personal data to a third
- 14 party as an asset that is part of a merger,
- 15 acquisition, bankruptcy, or other transaction in which
- 16 the third party assumes control of all or part of the
- 17 controller's assets.

18 "Sensitive data" means a category of personal data that
19 includes:

- 20 (1) Personal data revealing racial or ethnic origin,
- 21 religious beliefs, mental or physical health



1 diagnosis, sexual orientation, or citizenship or
2 immigration status;

3 (2) The processing of genetic or biometric data for the
4 purpose of uniquely identifying a natural person;

5 (3) The personal data collected from a known child; or

6 (4) Precise geolocation data.

7 "Targeted advertising" means displaying to a consumer
8 advertisements based on personal data obtained from that
9 consumer's activities over time and across non-affiliated
10 websites or online applications to predict the consumer's
11 preferences or interests. The term "targeted advertising" does
12 not include:

13 (1) Advertisements based on activities within a
14 controller's own websites or online applications;

15 (2) Advertisements based on the context of a consumer's
16 current search query, visit to a website, or online
17 application;

18 (3) Advertisements directed to a consumer in response to
19 the consumer's request for information or feedback; or



1 (4) Processing personal data processed solely for
2 measuring or reporting advertising performance, reach,
3 or frequency.

4 "Third party" means a natural or legal person, public
5 authority, agency, or body other than the consumer, controller,
6 processor, or an affiliate of the processor or the controller.

7 § -2 Scope; exemptions. (a) This chapter applies to
8 persons that conduct business in the State or produce products
9 or services that are targeted to residents of the State and:

10 (1) During a calendar year, control or process personal
11 data of at least one hundred thousand consumers; or

12 (2) Control or process personal data of at least twenty-
13 five thousand consumers and derive over fifty per cent
14 of gross revenue from the sale of personal data.

15 (b) This chapter shall not apply to any:

16 (1) Government entity;

17 (2) Financial institution or data subject to title V of
18 the Gramm-Leach-Bliley Act (Title 15 United States
19 Code chapter 94);

20 (3) Covered entity or business associate governed by the
21 privacy, security, and breach notification regulations



1 in Title 45 Code of Federal Regulations parts 160 and
2 164;

3 (4) Nonprofit organization; or

4 (5) Institution of higher education.

5 (c) The following information and data are exempt from
6 this chapter:

7 (1) Protected health information as defined in Title 45
8 Code of Federal Regulations section 160.103;

9 (2) Patient identifying information for purposes of
10 described in Title 42 United States Code section
11 290dd-2;

12 (3) Identifiable private information for purposes of the
13 protection of human subjects under Title 45 Code of
14 Federal Regulations part 46; identifiable private
15 information that is otherwise information collected as
16 part of human subjects research pursuant to the good
17 clinical practice guidelines issued by The
18 International Council for Harmonisation of Technical
19 Requirements for Pharmaceuticals for Human Use;
20 identifiable private information collected as part of
21 a clinical investigation under Title 21 Code of



- 1 Federal Regulations parts 50 and 56; personal data
2 used or shared in research conducted in accordance
3 with the requirements set forth in this chapter; and
4 other research conducted in accordance with applicable
5 law;
- 6 (4) Information and documents created for purposes of the
7 Health Care Quality Improvement Act of 1986 (Title 42
8 United States Code chapter 117);
- 9 (5) Patient safety work product for purposes of the
10 Patient Safety and Quality Improvement Act (Title 42
11 United States Code sections 299b-21 to 299b-26);
- 12 (6) Information derived from any of the health care-
13 related information listed in this subsection that is
14 de-identified in accordance with the requirements for
15 de-identification pursuant to the Health Insurance
16 Portability and Accountability Act;
- 17 (7) Information originating from, and intermingled to be
18 indistinguishable with, or information treated in the
19 same manner as information exempt under this
20 subsection that is maintained by a covered entity or
21 business associate as defined in the Health Insurance



- 1 Portability and Accountability Act or a program or a
2 qualified service organization as defined in Title 42
3 United States Code section 210dd-2;
- 4 (8) Information used only for public health activities and
5 purposes as authorized by the Health Insurance
6 Portability and Accountability Act;
- 7 (9) The collection, maintenance, disclosure, sale,
8 communication, or use of any personal information
9 bearing on a consumer's credit worthiness, credit
10 standing, credit capacity, character, general
11 reputation, personal characteristics, or mode of
12 living by a consumer reporting agency or furnisher
13 that provides information for use in a consumer
14 report, and by a user of a consumer report, but only
15 to the extent that the activity is regulated by and
16 authorized under the Fair Credit Reporting Act (Title
17 15 United States Code sections 1681 to 1681x);
- 18 (10) Personal data collected, processed, sold, or disclosed
19 in compliance with the Driver's Privacy Protection Act
20 of 1994 (Title 18 United States Code chapter 123);



- 1 (11) Personal data regulated by the Family Educational
- 2 Rights and Privacy Act (Title 20 United States Code
- 3 section 1232g);
- 4 (12) Personal data collected, processed, sold, or disclosed
- 5 in compliance with the Farm Credit Act of 1971, P.L.
- 6 92-181, as amended; and
- 7 (13) Data processed or maintained:
 - 8 (A) In the course of an individual applying to,
 - 9 employed by, or acting as an agent or independent
 - 10 contractor of a controller, processor, or third
 - 11 party, to the extent that the data is collected
 - 12 and used within the context of that role;
 - 13 (B) As the emergency contact information of an
 - 14 individual under this chapter used for emergency
 - 15 contact purposes; or
 - 16 (C) As necessary to retain to administer benefits for
 - 17 another individual relating to the individual
 - 18 under subparagraph (A) and used for the purposes
 - 19 of administering those benefits.
- 20 (d) Controllers and processors that comply with the
- 21 verifiable parental consent requirements of the Children's



1 Online Privacy Protection Act (Title 15 United States Code
2 chapter 91) shall be deemed compliant with any obligation to
3 obtain parental consent under this chapter.

4 § -3 Personal data rights; consumers. (a) A consumer
5 may invoke the consumer rights specified in this subsection at
6 any time by submitting a request to a controller specifying the
7 consumer rights the consumer wishes to invoke. A child's parent
8 or legal guardian may invoke the same consumer rights on behalf
9 of the child regarding processing personal data belonging to the
10 child. A controller shall comply with an authenticated consumer
11 request to exercise the right to:

12 (1) Confirm whether or not a controller is processing the
13 consumer's personal data and to access the personal
14 data;

15 (2) Correct inaccuracies in the consumer's personal data,
16 taking into account the nature of the personal data
17 and the purposes of the processing of the consumer's
18 personal data;

19 (3) Delete personal data provided by or obtained about the
20 consumer;



- 1 (4) Obtain a copy of the consumer's personal data that the
2 consumer previously provided to the controller in a
3 format that:
- 4 (A) Is portable;
 - 5 (B) To the extent technically feasible, is readily
6 usable; and
 - 7 (C) Allows the consumer to transmit the data to
8 another controller without hindrance, where the
9 processing is carried out by automated means;
- 10 (5) Opt out of the processing of the personal data for
11 purposes of:
- 12 (A) Targeted advertising;
 - 13 (B) The sale of personal data; or
 - 14 (C) Profiling in furtherance of decisions made by the
15 controller that profiling in furtherance of
16 decisions that produce legal or similar
17 significant effects concerning the consumer.
- 18 (b) Except as otherwise provided in this chapter, a
19 controller shall comply with a request by a consumer to exercise
20 the consumer rights specified in subsection (a) as follows:



- 1 (1) A controller shall respond to the consumer without
2 undue delay, but in all cases within forty-five days
3 of receipt of the request submitted pursuant to the
4 methods described in subsection (a). The response
5 period may be extended once by forty-five additional
6 days when reasonably necessary, taking into account
7 the complexity and number of the consumer's requests,
8 so long as the controller informs the consumer of the
9 extension within the initial forty-five-day response
10 period, together with the reason for the extension;
- 11 (2) If a controller declines to take action regarding the
12 consumer's request, the controller, without undue
13 delay, but no later than forty-five days of receipt of
14 the request, shall inform the consumer in writing of
15 the justification for declining to take action and
16 instructions for appealing the decision pursuant to
17 subsection (c);
- 18 (3) Information provided in response to a consumer request
19 shall be provided by a controller free of charge, up
20 to twice annually per consumer. If requests from a
21 consumer are manifestly unfounded, excessive, or



1 repetitive, the controller may charge the consumer a
2 reasonable fee to cover the administrative costs of
3 complying with the request or decline to act on the
4 request. The controller shall bear the burden of
5 demonstrating the manifestly unfounded, excessive, or
6 repetitive nature of the request;

7 (4) If a controller is unable to authenticate the request
8 using commercially reasonable efforts, the controller
9 shall not be required to comply with a request to
10 initiate an action under subsection (a) and may
11 request that the consumer provide additional
12 information reasonably necessary to authenticate the
13 consumer and the consumer's request; and

14 (5) A controller that has obtained personal data about a
15 consumer from a source other than the consumer shall
16 be deemed in compliance with a consumer's request to
17 delete the data pursuant to subsection (a)(3) by
18 either:

19 (A) Retaining a record of the deletion request and
20 the minimum data necessary for the purpose of
21 ensuring the consumer's personal data remains



1 deleted from the business's records and not using
2 the retained data for any other purpose pursuant
3 to the provisions of this chapter; or

4 (B) Opting the consumer out of the processing of the
5 personal data for any purpose except for those
6 exempted pursuant to the provisions of this
7 chapter.

8 (c) A controller shall establish a process for a consumer
9 to appeal the controller's refusal to take action on a request
10 within a reasonable period of time after the consumer's receipt
11 of the decision pursuant to subsection (b) (2); provided that the
12 appeal process shall be similar to the process for submitting
13 requests to initiate action pursuant to subsection (a). Within
14 sixty days of receipt of an appeal, a controller shall inform
15 the consumer in writing of its decision, including a written
16 explanation of the reasons for the decision. If the appeal is
17 denied, the controller shall also provide the consumer with an
18 online method, if available, or other method through which the
19 consumer may contact the department to submit a complaint.

20 § -4 Data controller responsibilities; transparency.

21 (a) A controller shall:



- 1 (1) Limit the collection of personal data to data that is
2 adequate, relevant, and reasonably necessary in
3 relation to the purposes for which the data is
4 processed, as disclosed to the consumer;
- 5 (2) Except as otherwise provided in this chapter, not
6 process personal data for purposes that are neither
7 reasonably necessary to nor compatible with the
8 disclosed purposes for which the personal data is
9 processed, as disclosed to the consumer, unless the
10 controller obtains the consumer's consent;
- 11 (3) Establish, implement, and maintain reasonable
12 administrative, technical, and physical data security
13 practices to protect the confidentiality, integrity,
14 and accessibility of personal data. The data security
15 practices shall be appropriate to the volume and
16 nature of the personal data at issue;
- 17 (4) Not process personal data in violation of state and
18 federal laws that prohibit unlawful discrimination
19 against consumers; and
- 20 (5) Not process sensitive data concerning a consumer
21 without obtaining the consumer's consent, or, in the



1 case of the processing of sensitive data concerning a
2 known child, without processing the data in accordance
3 with the Children's Online Privacy Protection Act
4 (Title 15 United States Code chapter 91).

5 (b) Any provision of a contract or agreement that purports
6 to waive or limit in any way consumer rights pursuant to
7 section -3 shall be deemed contrary to public policy and
8 shall be void and unenforceable.

9 (c) Controllers shall provide consumers with a reasonably
10 accessible, clear, and meaningful privacy notice that includes:

- 11 (1) The categories of personal data processed by the
12 controller;
- 13 (2) The purpose for processing personal data;
- 14 (3) How consumers may exercise their consumer rights
15 pursuant to section -3; including how a consumer
16 may appeal a controller's decision with regard to the
17 consumer's request;
- 18 (4) The categories of personal data that the controller
19 shares with third parties, if any; and
- 20 (5) The categories of third parties, if any, with whom the
21 controller shares personal data.



1 (d) If a controller sells personal data to third parties
2 or processes personal data for targeted advertising, the
3 controller shall clearly and conspicuously disclose the
4 processing, as well as the manner in which a consumer may
5 exercise the right to opt out of the processing.

6 (e) A controller shall establish, and shall describe in a
7 privacy notice, one or more secure and reliable means for
8 consumers to submit a request to exercise their consumer rights
9 under this chapter. Those means shall take into account the
10 ways in which consumers normally interact with the controller,
11 the need for secure and reliable communication of the requests,
12 and the ability of the controller to authenticate the identity
13 of the consumer making the request. Controllers shall not
14 require a consumer to create a new account in order to exercise
15 consumer rights pursuant to section 17-3 but may require a
16 consumer to use an existing account.

17 (f) A controller shall not discriminate against a consumer
18 for exercising any of the consumer rights contained in this
19 chapter, including denying goods or services, charging different
20 prices or rates for goods or services, or providing a different
21 level of quality of goods and services to the consumer; provided



1 that nothing in this chapter shall be construed to require a
2 controller to provide a product or service that requires the
3 personal data of a consumer that the controller does not collect
4 or maintain or to prohibit a controller from offering a
5 different price, rate, level, quality, or selection of goods or
6 services to a consumer, including offering goods or services for
7 no fee, if the consumer has exercised the consumer's right to
8 opt out pursuant to section -3 or the offer is related to a
9 consumer's voluntary participation in a bona fide loyalty,
10 rewards, premium features, discounts, or club card program.

11 **§ -5 Responsibility according to role; controller and**
12 **processor.** (a) In meeting its obligations under this chapter,
13 a processor shall adhere to the instructions of a controller and
14 shall assist the controller. The assistance shall include:

15 (1) Consideration of the nature of processing and the
16 information available to the processor, by appropriate
17 technical and organizational measures, insofar as this
18 is reasonably practicable, to fulfill the controller's
19 obligation to respond to consumer rights requests
20 pursuant to section -3;



1 (2) Consideration of account the nature of processing and
2 the information available to the processor, by
3 assisting the controller in meeting the controller's
4 obligations in relation to the security of processing
5 the personal data and in relation to the notice of
6 security breach pursuant to section 487N-2 in order to
7 meet the controller's obligations; and

8 (3) The provision of necessary information to enable the
9 controller to conduct and document data protection
10 assessments pursuant to section -6.

11 (b) A contract between a controller and a processor shall
12 govern the processor's data processing procedures with respect
13 to processing performed on behalf of the controller. The
14 contract shall be binding and clearly set forth instructions for
15 processing data, the nature and purpose of processing, the type
16 of data subject to processing, the duration of processing, and
17 the rights and obligations of both parties. The contract shall
18 also include requirements that the processor shall:

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



- 1 (2) At the controller's direction, delete or return all
2 personal data to the controller as requested at the
3 end of the provision of services, unless retention of
4 the personal data is required by law;
- 5 (3) Upon the reasonable request of the controller, make
6 available to the controller all information in its
7 possession necessary to demonstrate the processor's
8 compliance with the obligations in this chapter;
- 9 (4) Allow, and cooperate with, reasonable assessments by
10 the controller or the controller's designated
11 assessor; alternatively, the processor may arrange for
12 a qualified and independent assessor to conduct an
13 assessment of the processor's policies and technical
14 and organizational measures in support of the
15 obligations under this chapter using an appropriate
16 and accepted control standard or framework and
17 assessment procedure for the assessments. The
18 processor shall provide a report of the assessment to
19 the controller upon request; and
- 20 (5) Engage any subcontractor pursuant to a written
21 contract in accordance with subsection (c) that



1 requires the subcontractor to meet the obligations of
2 the processor with respect to the personal data.

3 (c) Nothing in this section shall be construed to relieve
4 a controller or a processor from the liabilities imposed on the
5 controller or processor by virtue of the controller's or
6 processor's role in the processing relationship as defined by
7 this chapter.

8 (d) A determination regarding whether a person is acting
9 as a controller or processor with respect to a specific
10 processing of data is a fact-based determination that depends
11 upon the context in which personal data is to be processed. A
12 processor that continues to adhere to a controller's
13 instructions with respect to a specific processing of personal
14 data remains a processor.

15 **§ -6 Data protection assessments.** (a) The data
16 protection assessment requirements of this section shall apply
17 to processing activities created or generated after January 1,
18 2024.

19 (b) A controller shall conduct and document a data
20 protection assessment of each of the following processing
21 activities involving personal data:



- 1 (1) The processing of personal data for purposes of
- 2 targeted advertising;
- 3 (2) The sale of personal data;
- 4 (3) The processing of personal data for purposes of
- 5 profiling, where the profiling presents a reasonably
- 6 foreseeable risk of:
- 7 (A) Unfair or deceptive treatment of, or unlawful
- 8 disparate impact on, consumers;
- 9 (B) Financial, physical, or reputational injury to
- 10 consumers;
- 11 (C) A physical intrusion or other intrusion upon the
- 12 solitude or seclusion, or the private affairs or
- 13 concerns, of consumers, where the intrusion would
- 14 be offensive to a reasonable person; or
- 15 (D) Other substantial injury to consumers;
- 16 (4) The processing of sensitive data; and
- 17 (5) Any processing activities involving personal data that
- 18 present a heightened risk of harm to consumers.
- 19 (c) Data protection assessments conducted pursuant to
- 20 subsection (b) shall identify and evaluate the benefits, direct
- 21 or indirect, that a controller, consumer, other stakeholders,



1 and the public may derive from processing against the potential
2 risks to the rights of consumers associated with the processing,
3 as mitigated by safeguards that can be employed by the
4 controller to reduce the risks. The use of de-identified data
5 and the reasonable expectations of consumers, as well as the
6 context of the processing and the relationship between the
7 controller and the consumer whose personal data is processed,
8 shall be factored into this assessment by the controller.

9 (d) The department may request, pursuant to a civil
10 investigative demand, that a controller disclose any data
11 protection assessment that is relevant to an investigation
12 conducted by the department, and the controller shall make the
13 data protection assessment available to the department. The
14 department may evaluate the data protection assessment for
15 compliance with the responsibilities set forth in section -4.
16 Data protection assessments shall be confidential and exempt
17 from public inspection and copying under chapter 92F. The
18 disclosure of a data protection assessment pursuant to a request
19 from the department shall not constitute a waiver of attorney-
20 client privilege or work product protection with respect to the
21 assessment and any information contained in the assessment.



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

4 (f) Data protection assessments conducted by a controller
5 for the purpose of compliance with other laws may comply under
6 this section if the assessments have a reasonably comparable
7 scope and effect.

8 § -7 Processing de-identified data; exemptions. (a)

9 The controller in possession of de-identified data shall:

- 10 (1) Take reasonable measures to ensure that the data
- 11 cannot be associated with a natural person;
- 12 (2) Publicly commit to maintaining and using de-identified
- 13 data without attempting to re-identify the data; and
- 14 (3) Contractually obligate any recipients of the
- 15 de-identified data to comply with all provisions of
- 16 this chapter.

17 (b) Nothing in this chapter shall be construed to require
18 a controller or processor to:

- 19 (1) Re-identify de-identified data or pseudonymous data;
- 20 or



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

5 (c) Nothing in this chapter shall be construed to require
6 a controller or processor to comply with an authenticated
7 consumer rights request pursuant to section -3 if all of the
8 following are true:

9 (1) The controller is not reasonably capable of
10 associating the request with the personal data or it
11 would be unreasonably burdensome for the controller to
12 associate the request with the personal data;

13 (2) The controller does not use the personal data to
14 recognize or respond to the specific consumer who is
15 the subject of the personal data, or associate the
16 personal data with other personal data about the same
17 specific consumer; and

18 (3) The controller does not sell the personal data to any
19 third party or otherwise voluntarily disclose the
20 personal data to any third party other than a



1 processor, except as otherwise permitted in this
2 section.

3 (d) The consumer rights specified in section -3(a)(1)
4 to (4) and section -4 shall not apply to pseudonymous data in
5 cases in which the controller is able to demonstrate that any
6 information necessary to identify the consumer is kept
7 separately and is subject to effective technical and
8 organizational controls that prevent the controller from
9 accessing the information.

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

16 § -8. Limitations. (a) Nothing in this chapter shall be
17 construed to restrict a controller's or processor's ability to:

18 (1) Comply with federal, state, or local laws, rules, or
19 regulations;



- 1 (2) Comply with a civil, criminal, or regulatory inquiry,
2 investigation, subpoena, or summons by federal, state,
3 county, or other governmental authorities;
- 4 (3) Cooperate with law enforcement agencies concerning
5 conduct or activity that the controller or processor
6 reasonably and in good faith believes may violate
7 federal, state, or county laws, rules, or regulations;
- 8 (4) Investigate, establish, exercise, prepare for, or
9 defend legal claims;
- 10 (5) Provide a product or service specifically requested by
11 a consumer, perform a contract to which the consumer
12 is a party, including fulfilling the terms of a
13 written warranty, or take steps at the request of the
14 consumer before entering into a contract;
- 15 (6) Take immediate steps to protect an interest that is
16 essential for the life or physical safety of the
17 consumer or of another natural person, and where the
18 processing cannot be manifestly based on another legal
19 basis;
- 20 (7) Prevent, detect, protect against, or respond to
21 security incidents, identity theft, fraud, harassment,



1 malicious or deceptive activities, or any illegal
2 activity; preserve the integrity or security of
3 systems; or investigate, report, or prosecute those
4 responsible for any of those actions;

5 (8) Engage in public or peer-reviewed scientific or
6 statistical research in the public interest that
7 adheres to all other applicable ethics and privacy
8 laws and is approved, monitored, and governed by an
9 independent oversight entity that determines:

10 (A) If the deletion of the information is likely to
11 provide substantial benefits that do not
12 exclusively accrue to the controller;

13 (B) The expected benefits of the research outweigh
14 the privacy risks; and

15 (C) If the controller has implemented reasonable
16 safeguards to mitigate privacy risks associated
17 with research, including any risks associated
18 with reidentification; or

19 (9) Assist another controller, processor, or third party
20 with any of the obligations under this subsection.



1 (b) The obligations imposed on controllers or processors
2 under this chapter shall not restrict a controller's or
3 processor's ability to collect, use, or retain data to:

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

6 (2) Effectuate a product recall;

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

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

18 (c) The obligations imposed on controllers or processors
19 under this chapter shall not apply where compliance by the
20 controller or processor with this chapter would violate an
21 evidentiary privilege under state law. Nothing in this chapter



1 shall be construed to prevent a controller or processor from
2 providing personal data concerning a consumer to a person
3 covered by an evidentiary privilege under state law as part of a
4 privileged communication.

5 (d) A controller or processor that discloses personal data
6 to a third-party controller or processor, in compliance with the
7 requirements of this chapter, shall not be deemed to be in
8 violation of this chapter if the third-party controller or
9 processor that receives and processes the personal data is in
10 violation of this chapter; provided that, at the time of the
11 disclosure of the personal data, the disclosing controller or
12 processor did not have actual knowledge that the recipient
13 intended to commit a violation. A third-party controller or
14 processor that receives personal data from a controller or
15 processor in compliance with the requirements of this chapter
16 shall not be deemed to be in violation of this chapter if the
17 controller or processor from which the third-party controller or
18 processor receives the personal data is in violation of this
19 chapter.

20 (e) Nothing in this chapter shall be construed to:



- 1 (1) Impose an obligation on controllers and processors
2 that adversely affects the rights or freedoms of any
3 person, including the right of free expression
4 pursuant to the First Amendment to the Constitution of
5 the United States; or
- 6 (2) Apply to the processing of personal data by a person
7 in the course of a purely personal or household
8 activity.
- 9 (f) Personal data processed by a controller pursuant to
10 this section shall not be processed for any purpose other than
11 those expressly listed in this section unless otherwise allowed
12 by this chapter. Personal data processed by a controller
13 pursuant to this section may be processed to the extent that the
14 processing is:
- 15 (1) Reasonably necessary and proportionate to the purposes
16 listed in this section; and
- 17 (2) Adequate, relevant, and limited to what is necessary
18 in relation to the specific purposes listed in this
19 section. Personal data collected, used, or retained
20 pursuant to subsection (b) where applicable, shall
21 consider the nature and purpose or purposes of the



1 collection, use, or retention. The data shall be
2 subject to reasonable administrative, technical, and
3 physical measures to protect the confidentiality,
4 integrity, and accessibility of the personal data and
5 to reduce reasonably foreseeable risks of harm to
6 consumers relating to the collection, use, or
7 retention of personal data.

8 (g) If a controller processes personal data pursuant to an
9 exemption in this section, the controller bears the burden of
10 demonstrating that the processing qualifies for the exemption
11 and complies with subsection (f).

12 (h) An entity's processing of personal data for the
13 purposes expressly identified in subsection (a) shall not be the
14 sole basis for the department to consider the entity as a
15 controller with respect to the processing.

16 **§ -9 Investigative authority; civil investigative**
17 **demand.** (a) Whenever the department has reasonable cause to
18 believe that any person has engaged in, is engaging in, or is
19 about to engage in any violation of this chapter, the department
20 may either require or permit the person to file with the
21 department a statement in writing or otherwise, under oath, as



1 to all facts and circumstances concerning the subject matter.
2 The department may also require any other data and information
3 as the department may deem relevant to the subject matter of an
4 investigation of a possible violation of this chapter and may
5 make special and independent investigations as the department
6 may deem necessary in connection with the matter.

7 (b) In connection with the investigation, the department
8 may issue a subpoena to witnesses by which the department may:

- 9 (1) Compel the attendance of the witnesses;
- 10 (2) Examine the witnesses under oath before the department
11 or a court of record;
- 12 (3) Subject to subsection (d), require the production of
13 any books or papers that the department deems relevant
14 or material to the inquiry; and
- 15 (4) Issue written interrogatories to be answered by the
16 witness served or, if the witness served is a
17 corporation, partnership, association, governmental
18 agency, or any person other than a natural person, by
19 any officer or agent, who shall furnish the
20 information as is available to the witness.



1 The investigative powers of this subsection shall not abate
2 or terminate by reason of any action or proceeding brought by
3 the department under this chapter.

4 (c) When documentary material is demanded by subpoena, the
5 subpoena shall not:

6 (1) Contain any requirement that would be unreasonable or
7 improper if contained in a subpoena duces tecum issued
8 by a court of the State; or

9 (2) Require the disclosure of any documentary material
10 that would be privileged, or production of which for
11 any other reason would not be required by a subpoena
12 duces tecum issued by a court of the State.

13 (d) Where the information requested pursuant to a civil
14 investigative demand may be derived or ascertained from the
15 business records of the party upon whom the interrogatory has
16 been served or from an examination, audit, or inspection of the
17 business records, or from a compilation, abstract, or summary
18 based therein, and the burden of deriving or ascertaining the
19 answer is substantially the same for the department as for the
20 party from whom the information is requested, it shall be
21 sufficient for that party to specify the records from which the



1 answer may be derived or ascertained and to afford the
2 department, or other individuals properly designated by the
3 department, reasonable opportunity to examine, audit, or inspect
4 the records and to make copies, compilations, abstracts, or
5 summaries. Further, the department may elect to require the
6 production pursuant to this section of documentary material
7 before or after the taking of any testimony of the person
8 summoned pursuant to a subpoena; in which event, the documentary
9 matter shall be made available for inspection and copying during
10 normal business hours at the principal place of business of the
11 person served, or at any other time and place, as may be agreed
12 upon by the person served and the department.

13 (e) Any subpoena issued by the department shall contain
14 the following information:

- 15 (1) The statute alleged to have been violated and the
16 subject matter of the investigation;
- 17 (2) The date, place, time, and locations at which the
18 person is required to appear to produce documentary
19 material in the person's possession, custody, or
20 control; provided that the date shall not be less than
21 twenty days after the date of the subpoena; and



1 (3) If documentary material is required to be produced, it
2 shall be described by class so as to clearly indicate
3 the material demanded.

4 (f) Service of subpoena of the department may be made by:

5 (1) Delivery of a duly executed copy to the person served,
6 or if a person is not a natural person, to the
7 principal place of business of the person to be
8 served; or

9 (2) Mailing by certified mail, return receipt requested,
10 of a duly executed copy addressed to the person to be
11 served at the person's principal place of business in
12 the State, or if the person has no place of business
13 in the State, to the person's office.

14 (g) Within twenty days after the service of a demand upon
15 any person or enterprise, or at any time before the return date
16 specified in the demand, whichever period is shorter, the party
17 may file in the circuit court and serve upon the attorney
18 general a petition for an order modifying or setting aside the
19 demand. The time allowed for compliance with the demand in
20 whole or in part as deemed proper and ordered by the court shall
21 not run during the pendency of the petition in the court. The



1 petition shall specify each ground upon which the petitioner
2 relies in seeking relief, and may be based upon any failure of
3 the demand to comply with the provisions of this chapter or upon
4 any constitutional or other legal right or privilege of the
5 party. This subsection shall be the exclusive means for a
6 witness summoned pursuant to a subpoena pursuant to this section
7 to challenge the subpoena.

8 (h) The examination of all witnesses under this section
9 shall be conducted by the attorney general, or the attorney
10 general's designee, before a person authorized to administer
11 oaths in the State. The testimony shall be taken
12 stenographically or by a sound recording device and shall be
13 transcribed.

14 (i) Any person required to testify or to submit
15 documentary evidence shall be entitled, on payment of lawfully
16 prescribed cost, to procure a copy of any document produced by
17 the person and of the person's own testimony as stenographically
18 reported or, in the case of depositions, as reduced to writing
19 by or under the direction of a person taking the deposition.
20 Any party compelled to testify or to produce documentary
21 evidence may be accompanied and advised by counsel, but counsel



1 may not, as a matter of right, otherwise participate in the
2 investigation.

3 (j) Any persons served with a subpoena by the department
4 under this chapter, other than any person whose conduct or
5 practices are being investigated or any officer, director, or
6 person in the employ of the person under investigation, shall be
7 paid the same fees and mileage as paid witnesses in the courts
8 of the State. No person shall be excused from attending an
9 inquiry pursuant to the mandate of a subpoena, or from producing
10 a paper, or from being examined or required to answer questions
11 on the ground of failure to tender or pay a witness fee or
12 mileage.

13 (k) Any natural person who shall neglect or refuse to
14 attend and testify, or to answer any lawful inquiry or to
15 produce documentary evidence, if in the person's power to do so,
16 in obedience of a subpoena or lawful request of the department
17 or those properly authorized by the department, pursuant to this
18 section, shall be guilty of a misdemeanor.

19 (l) Any natural person who commits perjury or false
20 swearing or contempt in answering, failing to answer, producing
21 evidence, or failing to produce evidence in accordance with a



1 subpoena or lawful request by the department, pursuant to this
2 section, shall be guilty of a misdemeanor.

3 (m) In any investigation brought by the department
4 pursuant to this chapter, no person shall be excused from
5 attending, testifying, or producing documentary material,
6 objects, or intangible things in obedience to a subpoena under
7 order of the court on the ground that the testimony or evidence
8 required of the person may tend to incriminate the person or
9 subject the person to any penalty; provided that no testimony or
10 other information compelled either by the department or under
11 order of a court, or any information directly or indirectly
12 derived from the testimony or other information, may be used
13 against the individual or witness in any criminal case. A
14 person may be prosecuted or subjected to penalty or forfeiture
15 for any perjury, false swearing, or contempt committed in
16 answering, or failing to answer, or in producing evidence or
17 failing to do so in accordance with the order of the department
18 or a court. If a person refuses to testify or produce evidence
19 after being granted immunity from prosecution and after being
20 ordered to testify or produce evidence, the person may be
21 adjudged in contempt by a court pursuant to section 710-1077.



1 This subsection shall not be construed to prevent the department
2 from instituting other appropriate contempt proceedings against
3 any person who violates this section.

4 (n) Any state or county public official, deputy,
5 assistant, clerk, subordinate, or employees, and all other
6 persons shall render and furnish to the department, when so
7 requested, all information and assistance in the person's
8 possession or within the person's power. Any officer
9 participating in the inquiry and any person examined as a
10 witness upon the inquiry who shall disclose to any person other
11 than the department, the name of any witness examined or any
12 other information obtained upon the inquiry, except as so
13 directed by the department, shall be guilty of a misdemeanor.

14 (o) The department shall maintain the secrecy of all
15 evidence, testimony, documents, or other results of
16 investigations; provided that:

17 (1) The department may disclose any investigative evidence
18 to any federal or state law enforcement authority that
19 has restrictions governing confidentiality similar to
20 those contained in this subsection;



1 (2) The department may present and disclose any
2 investigative evidence in any action or proceeding
3 brought by the department under this chapter; and

4 (3) Any upon written authorization of the attorney
5 general, an inquiry under this section may be made
6 public.

7 Violation of this subsection shall be a misdemeanor.

8 § -10 Enforcement; private right of action. (a) Any
9 violation of this chapter shall constitute an unfair method of
10 competition and unfair and deceptive acts or practices in the
11 conduct of any trade or commerce under section 480-2 and shall
12 be subject to a civil penalty as provided in section 480-3.1.

13 (b) Any consumer injured by a violation of this chapter
14 may bring a civil action against a controller or processor
15 pursuant to section 480-2.

16 § -11 Rules. The department shall adopt rules, pursuant
17 to chapter 91, necessary for the purposes of this chapter."

18 SECTION 2. This Act does not affect rights and duties that
19 matured, penalties that were incurred, and proceedings that were
20 begun before its effective date.



1 SECTION 3. This Act shall take effect on July 1, 2023.

2

INTRODUCED BY: *Alan Bir*

JAN 25 2023



H.B. NO. 1497

Report Title:

Consumers; Data; Privacy; Attorney General; Appropriation

Description:

Establishes a framework to regulate controllers and processors with access to personal consumer data. Establishes that a violation of the consumer data privacy act constitutes an unfair method of competition and unfair and deceptive acts or practices in the conduct of any trade of commerce. Authorizes a person injured by a violation of the personal consumer data act to bring a civil action against a controller or processor.

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.

