

JAN 21 2022

---

# 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 sixteen years  
5 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 "Fund" means the consumer privacy special fund established  
6 pursuant to section -11.

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

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

12 "Institution of higher education" means:

13 (1) The University of Hawaii system, or one of its  
14 campuses; or

15 (2) A private college or university authorized to operate  
16 in the State pursuant to chapter 305J.

17 "Nonprofit organization" means any:

18 (1) Corporation incorporated pursuant to chapter 414D;

19 (2) Organization exempt from taxation under section  
20 501(c)(3), (6), or (12) of the Internal Revenue Code  
21 of 1986, as amended; or



1           (3) Electric utility cooperative association subject to  
2           chapter 421C.

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

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

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



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

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

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

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



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

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

4 (1) The disclosure of personal data to a processor that  
5 processes the personal data on behalf of the  
6 controller;

7 (2) The disclosure of personal data to a third party for  
8 purposes of providing a product or service requested  
9 by the consumer;

10 (3) The disclosure or transfer of personal data to an  
11 affiliate of the controller;

12 (4) The disclosure of information that the consumer:

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

15 (B) Did not restrict to a specific audience; or

16 (5) The disclosure or transfer of personal data to a third  
17 party as an asset that is part of a merger,  
18 acquisition, bankruptcy, or other transaction in which  
19 the third party assumes control of all or part of the  
20 controller's assets.



1 "Sensitive data" means a category of personal data that  
2 includes:

3 (1) Personal data revealing racial or ethnic origin,  
4 religious beliefs, mental or physical health  
5 diagnosis, sexual orientation, or citizenship or  
6 immigration status;

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

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

10 (4) Precise geolocation data.

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

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

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





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

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

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

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

(1) During a calendar year, control or process personal data of at least consumers; or

(2) Control or process personal data of at least consumers and derive over fifty per cent of gross revenue from the sale of personal data.

(b) This chapter shall not apply to any:

(1) Government entity;

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



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

3 (3) Nonprofit organization; or

4 (4) 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) Nonpublic personal information, as defined in the  
10 Gramm-Leach-Bliley Act (15 U.S.C. chapter 94);

11 (3) Confidential rewards described in title 42 United  
12 States Code section 290dd-2;

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



1 a clinical investigation under title 21 Code of  
2 Federal Regulations parts 50 and 56; personal data  
3 used or shared in research conducted in accordance  
4 with the requirements set forth in this chapter; and  
5 other research conducted in accordance with applicable  
6 law;

7 (5) Information and documents created for purposes of the  
8 Health Care Quality Improvement Act of 1986 (42 U.S.C.  
9 chapter 117);

10 (6) Patient safety work product for purposes of the  
11 Patient Safety and Quality Improvement Act (42 U.S.C.  
12 sections 299b-21 to 299b-26);

13 (7) Information derived from any of the health care-  
14 related information listed in this subsection that is  
15 de-identified in accordance with the requirements for  
16 de-identification pursuant to the Health Insurance  
17 Portability and Accountability Act;

18 (8) Information originating from, and intermingled to be  
19 indistinguishable with, or information treated in the  
20 same manner as information exempt under this  
21 subsection that is maintained by a covered entity or



1 business associate as defined in the Health Insurance  
2 Portability and Accountability Act or a program or a  
3 qualified service organization as defined in title 42  
4 Code of Federal Regulations section 2.11;

5 (9) Information used only for public health activities and  
6 purposes as authorized by the Health Insurance  
7 Portability and Accountability Act;

8 (10) The collection, maintenance, disclosure, sale,  
9 communication, or use of any personal information  
10 bearing on a consumer's credit worthiness, credit  
11 standing, credit capacity, character, general  
12 reputation, personal characteristics, or mode of  
13 living by a consumer reporting agency or furnisher  
14 that provides information for use in a consumer  
15 report, and by a user of a consumer report, but only  
16 to the extent that the activity is regulated by and  
17 authorized under the Fair Credit Reporting Act (15  
18 U.S.C. sections 1681 to 1681x);

19 (11) Personal data collected, processed, sold, or disclosed  
20 in compliance with the Driver's Privacy Protection Act  
21 of 1994 (18 U.S.C. chapter 123);



1 (12) Personal data regulated by the Family Educational  
2 Rights and Privacy Act (20 U.S.C. section 1232g);

3 (13) Personal data collected, processed, sold, or disclosed  
4 in compliance with the Farm Credit Act of 1971, P.L.  
5 92-181, as amended; and

6 (14) Data processed or maintained:

7 (A) In the course of an individual applying to,  
8 employed by, or acting as an agent or independent  
9 contractor of a controller, processor, or third  
10 party, to the extent that the data is collected  
11 and used within the context of that role;

12 (B) As the emergency contact information of an  
13 individual under this chapter used for emergency  
14 contact purposes; or

15 (C) As necessary to retain to administer benefits for  
16 another individual relating to the individual  
17 under subparagraph (A) and used for the purposes  
18 of administering those benefits.

19 (d) Controllers and processors that comply with the  
20 verifiable parental consent requirements of the Children's  
21 Online Privacy Protection Act (15 U.S.C. chapter 91) shall be



1 deemed compliant with any obligation to obtain parental consent  
2 under this chapter.

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

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

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

18       (3) To delete personal data provided by or obtained about  
19           the consumer;



1           (4) To obtain a copy of the consumer's personal data that  
2           the consumer previously provided to the controller in  
3           a 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) To 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 results in the provision or  
16          denial by the controller of financial and lending  
17          services, housing, insurance, education  
18          enrollment, criminal justice, employment  
19          opportunities, health care services, or access to  
20          basic necessities, including food and water.



1           (b) Except as otherwise provided in this chapter, a  
2 controller shall comply with a request by a consumer to exercise  
3 the consumer rights specified in subsection (a) as follows:

4           (1) A controller shall respond to the consumer without  
5 undue delay, but in all cases within forty-five days  
6 of receipt of the request submitted pursuant to the  
7 methods described in subsection (a). The response  
8 period may be extended once by forty-five additional  
9 days when reasonably necessary, taking into account  
10 the complexity and number of the consumer's requests,  
11 so long as the controller informs the consumer of the  
12 extension within the initial forty-five-day response  
13 period, together with the reason for the extension;

14          (2) If a controller declines to take action regarding the  
15 consumer's request, the controller, without undue  
16 delay, but no later than forty-five days of receipt of  
17 the request, shall inform the consumer in writing of  
18 the justification for declining to take action and  
19 instructions for appealing the decision pursuant to  
20 subsection (c);





1           (3) Information provided in response to a consumer request  
2           shall be provided by a controller free of charge, up  
3           to twice annually per consumer. If requests from a  
4           consumer are manifestly unfounded, excessive, or  
5           repetitive, the controller may charge the consumer a  
6           reasonable fee to cover the administrative costs of  
7           complying with the request or decline to act on the  
8           request. The controller shall bear the burden of  
9           demonstrating the manifestly unfounded, excessive, or  
10          repetitive nature of the request; and

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

18          (c) A controller shall establish a process for a consumer  
19          to appeal the controller's refusal to take action on a request  
20          within a reasonable period of time after the consumer's receipt  
21          of the decision pursuant to subsection (b)(2); provided that the



1 appeal process shall be similar to the process for submitting  
2 requests to initiate action pursuant to subsection (a). Within  
3 sixty days of receipt of an appeal, a controller shall inform  
4 the consumer in writing of its decision, including a written  
5 explanation of the reasons for the decision. If the appeal is  
6 denied, the controller shall also provide the consumer with an  
7 online method, if available, or other method through which the  
8 consumer may contact the department to submit a complaint.

9       **§ -4 Data controller responsibilities; transparency.**

10       (a) A controller shall:

11           (1) Limit the collection of personal data to data that is  
12               adequate, relevant, and reasonably necessary in  
13               relation to the purposes for which the data is  
14               processed, as disclosed to the consumer;

15           (2) Except as otherwise provided in this chapter, not  
16               process personal data for purposes that are neither  
17               reasonably necessary to nor compatible with the  
18               disclosed purposes for which the personal data is  
19               processed, as disclosed to the consumer, unless the  
20               controller obtains the consumer's consent;



1       (3) Establish, implement, and maintain reasonable  
2       administrative, technical, and physical data security  
3       practices to protect the confidentiality, integrity,  
4       and accessibility of personal data. The data security  
5       practices shall be appropriate to the volume and  
6       nature of the personal data at issue;

7       (4) Not process personal data in violation of state and  
8       federal laws that prohibit unlawful discrimination  
9       against consumers; and

10      (5) Not process sensitive data concerning a consumer  
11      without obtaining the consumer's consent, or, in the  
12      case of the processing of sensitive data concerning a  
13      known child, without processing the data in accordance  
14      with the Children's Online Privacy Protection Act (15  
15      U.S.C. chapter 91).

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

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



1           (1) The categories of personal data processed by the  
2           controller;

3           (2) The purpose for processing personal data;

4           (3) How consumers may exercise their consumer rights  
5           pursuant to section -3, including how a consumer  
6           may appeal a controller's decision with regard to the  
7           consumer's request;

8           (4) The categories of personal data that the controller  
9           shares with third parties, if any; and

10          (5) The categories of third parties, if any, with whom the  
11          controller shares personal data.

12          (d) If a controller sells personal data to third parties  
13 or processes personal data for targeted advertising, the  
14 controller shall clearly and conspicuously disclose the  
15 processing, as well as the manner in which a consumer may  
16 exercise the right to opt out of the processing.

17          (e) A controller shall establish, and shall describe in a  
18 privacy notice, one or more secure and reliable means for  
19 consumers to submit a request to exercise their consumer rights  
20 under this chapter. Those means shall take into account the  
21 ways in which consumers normally interact with the controller,



1 the need for secure and reliable communication of the requests,  
2 and the ability of the controller to authenticate the identity  
3 of the consumer making the request. Controllers shall not  
4 require a consumer to create a new account in order to exercise  
5 consumer rights pursuant to section -3 but may require a  
6 consumer to use an existing account.

7 (f) A controller shall not discriminate against a consumer  
8 for exercising any of the consumer rights contained in this  
9 chapter, including denying goods or services, charging different  
10 prices or rates for goods or services, or providing a different  
11 level of quality of goods and services to the consumer; provided  
12 that nothing in this chapter shall be construed to require a  
13 controller to provide a product or service that requires the  
14 personal data of a consumer that the controller does not collect  
15 or maintain or to prohibit a controller from offering a  
16 different price, rate, level, quality, or selection of goods or  
17 services to a consumer, including offering goods or services for  
18 no fee, if the consumer has exercised the consumer's right to  
19 opt out pursuant to section -3 or the offer is related to a  
20 consumer's voluntary participation in a bona fide loyalty,  
21 rewards, premium features, discounts, or club card program.



1       §   -5   Responsibility according to role; controller and  
2   processor. (a) In meeting its obligations under this chapter,  
3   a processor shall adhere to the instructions of a controller and  
4   shall assist the controller. The assistance shall include:

5       (1) Consideration of the nature of processing and the  
6           information available to the processor, by appropriate  
7           technical and organizational measures, insofar as this  
8           is reasonably practicable, to fulfill the controller's  
9           obligation to respond to consumer rights requests  
10          pursuant to section   -3;

11       (2) Consideration of account the nature of processing and  
12          the information available to the processor, by  
13          assisting the controller in meeting the controller's  
14          obligations in relation to the security of processing  
15          the personal data and in relation to the notice of  
16          security breach pursuant to section 487N-2 in order to  
17          meet the controller's obligations; and

18       (3) The provision of necessary information to enable the  
19          controller to conduct and document data protection  
20          assessments pursuant to section   -6.



1           (b) A contract between a controller and a processor shall  
2 govern the processor's data processing procedures with respect  
3 to processing performed on behalf of the controller. The  
4 contract shall be binding and clearly set forth instructions for  
5 processing data, the nature and purpose of processing, the type  
6 of data subject to processing, the duration of processing, and  
7 the rights and obligations of both parties. The contract shall  
8 also include requirements that the processor shall:

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

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

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

20          (4) Allow, and cooperate with, reasonable assessments by  
21               the controller or the controller's designated



1           assessor; alternatively, the processor may arrange for  
2           a qualified and independent assessor to conduct an  
3           assessment of the processor's policies and technical  
4           and organizational measures in support of the  
5           obligations under this chapter using an appropriate  
6           and accepted control standard or framework and  
7           assessment procedure for the assessments. The  
8           processor shall provide a report of the assessment to  
9           the controller upon request; and

10       (5) Engage any subcontractor pursuant to a written  
11       contract in accordance with subsection (c) that  
12       requires the subcontractor to meet the obligations of  
13       the processor with respect to the personal data.

14       (c) Nothing in this section shall be construed to relieve  
15       a controller or a processor from the liabilities imposed on the  
16       controller or processor by virtue of the controller's or  
17       processor's role in the processing relationship as defined by  
18       this chapter.

19       (d) A determination regarding whether a person is acting  
20       as a controller or processor with respect to a specific  
21       processing of data is a fact-based determination that depends





1 upon the context in which personal data is to be processed. A  
2 processor that continues to adhere to a controller's  
3 instructions with respect to a specific processing of personal  
4 data remains a processor.

5       **§ -6 Data protection assessments.** (a) The data  
6 protection assessment requirements of this section shall apply  
7 to processing activities created or generated after January 1,  
8 2024.

9       (b) A controller shall conduct and document a data  
10 protection assessment of each of the following processing  
11 activities involving personal data:

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

14       (2) The sale of personal data;

15       (3) The processing of personal data for purposes of  
16           profiling, where the profiling presents a reasonably  
17           foreseeable risk of:

18           (A) Unfair or deceptive treatment of, or unlawful  
19           disparate impact on, consumers;

20           (B) Financial, physical, or reputational injury to  
21           consumers;



1 (C) A physical intrusion or other intrusion upon the  
2 solitude or seclusion, or the private affairs or  
3 concerns, of consumers, where the intrusion would  
4 be offensive to a reasonable person; or

5 (D) Other substantial injury to consumers;

6 (4) The processing of sensitive data; and

7 (5) Any processing activities involving personal data that  
8 present a heightened risk of harm to consumers.

9 (c) Data protection assessments conducted pursuant to  
10 subsection (b) shall identify and evaluate the benefits, direct  
11 or indirect, that a controller, consumer, other stakeholders,  
12 and the public may derive from processing against the potential  
13 risks to the rights of consumers associated with the processing,  
14 as mitigated by safeguards that can be employed by the  
15 controller to reduce the risks. The use of de-identified data  
16 and the reasonable expectations of consumers, as well as the  
17 context of the processing and the relationship between the  
18 controller and the consumer whose personal data is processed,  
19 shall be factored into this assessment by the controller.

20 (d) The department may request, pursuant to a civil  
21 investigative demand, that a controller disclose any data



1 protection assessment that is relevant to an investigation  
2 conducted by the department, and the controller shall make the  
3 data protection assessment available to the department. The  
4 department may evaluate the data protection assessment for  
5 compliance with the responsibilities set forth in section -4.  
6 Data protection assessments shall be confidential and exempt  
7 from public inspection and copying under chapter 92F. The  
8 disclosure of a data protection assessment pursuant to a request  
9 from the department shall not constitute a waiver of attorney-  
10 client privilege or work product protection with respect to the  
11 assessment and any information contained in the assessment.

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

15 (f) Data protection assessments conducted by a controller  
16 for the purpose of compliance with other laws may comply under  
17 this section if the assessments have a reasonably comparable  
18 scope and effect.

19 **§ -7 Processing de-identified data; exemptions.** (a)

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



1 (1) Take reasonable measures to ensure that the data  
2 cannot be associated with a natural person;

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

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

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

10 (1) Re-identify de-identified data or pseudonymous data;  
11 or

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

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

20 (1) The controller is not reasonably capable of  
21 associating the request with the personal data or it



1           would be unreasonably burdensome for the controller to  
2           associate the request with the personal data;

3           (2) The controller does not use the personal data to  
4           recognize or respond to the specific consumer who is  
5           the subject of the personal data, or associate the  
6           personal data with other personal data about the same  
7           specific consumer; and

8           (3) The controller does not sell the personal data to any  
9           third party or otherwise voluntarily disclose the  
10          personal data to any third party other than a  
11          processor, except as otherwise permitted in this  
12          section.

13          (d) The consumer rights specified in section     -3(a)(1)  
14   to (4) and section     -4 shall not apply to pseudonymous data in  
15   cases in which the controller is able to demonstrate that any  
16   additional information necessary to identify the consumer is  
17   kept separately and is subject to effective technical and  
18   organizational controls that:

19          (1) Ensure that the personal data is not attributed to an  
20               identified or identifiable natural person; and

21          (2) Prevent the controller from accessing the information.



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

7 **§ -8 Limitations.** (a) Nothing in this chapter shall be  
8 construed to restrict a controller's or processor's ability to:

9 (1) Comply with federal, state, or local laws, rules, or  
10 regulations;

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

14 (3) Cooperate with law enforcement agencies concerning  
15 conduct or activity that the controller or processor  
16 reasonably and in good faith believes may violate  
17 federal, state, or county laws, rules, or regulations;

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

20 (5) Provide a product or service specifically requested by  
21 a consumer, perform a contract to which the consumer



1 is a party, including fulfilling the terms of a  
2 written warranty, or take steps at the request of the  
3 consumer before entering into a contract;

4 (6) Take immediate steps to protect an interest that is  
5 essential for the life or physical safety of the  
6 consumer or of another natural person, and where the  
7 processing cannot be manifestly based on another legal  
8 basis;

9 (7) Prevent, detect, protect against, or respond to  
10 security incidents, identity theft, fraud, harassment,  
11 malicious or deceptive activities, or any illegal  
12 activity; preserve the integrity or security of  
13 systems; or investigate, report, or prosecute those  
14 responsible for any of those actions;

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



1 (A) If the deletion of the information is likely to  
2 provide substantial benefits that do not  
3 exclusively accrue to the controller;

4 (B) The expected benefits of the research outweigh  
5 the privacy risks; and

6 (C) If the controller has implemented reasonable  
7 safeguards to mitigate privacy risks associated  
8 with research, including any risks associated  
9 with reidentification; or

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

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

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

17 (2) Effectuate a product recall;

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

20 (4) Perform internal operations that are reasonably  
21 aligned with the expectations of the consumer,





1 reasonably anticipated based on the consumer's  
2 existing relationship with the controller, or are  
3 otherwise compatible with processing data in  
4 furtherance of the provision of a product or service  
5 specifically requested by a consumer or the  
6 performance of a contract to which the consumer is a  
7 party.

8 (c) The obligations imposed on controllers or processors  
9 under this chapter shall not apply where compliance by the  
10 controller or processor with this chapter would violate an  
11 evidentiary privilege under state law. Nothing in this chapter  
12 shall be construed to prevent a controller or processor from  
13 providing personal data concerning a consumer to a person  
14 covered by an evidentiary privilege under state law as part of a  
15 privileged communication.

16 (d) A controller or processor that discloses personal data  
17 to a third-party controller or processor in compliance with the  
18 requirements of this chapter shall not be deemed to be in  
19 violation of this chapter if the third-party controller or  
20 processor that receives and processes the personal data is in  
21 violation of this chapter; provided that, at the time of the



1 disclosure of the personal data, the disclosing controller or  
2 processor did not have actual knowledge that the recipient  
3 intended to commit a violation. A third-party controller or  
4 processor that receives personal data from a controller or  
5 processor in compliance with the requirements of this chapter  
6 shall not be deemed to be in violation of this chapter if the  
7 controller or processor from which the third-party controller or  
8 processor receives the personal data is in violation of this  
9 chapter.

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

11 (1) Impose an obligation on controllers and processors  
12 that adversely affects the rights or freedoms of any  
13 person, including the right of free expression  
14 pursuant to the First Amendment to the Constitution of  
15 the United States; or

16 (2) Apply to the processing of personal data by a person  
17 in the course of a purely personal or household  
18 activity.

19 (f) Personal data processed by a controller pursuant to  
20 this section shall not be processed for any purpose other than  
21 those expressly listed in this section unless otherwise allowed



1 by this chapter. Personal data processed by a controller  
2 pursuant to this section may be processed to the extent that the  
3 processing is:

4 (1) Reasonably necessary and proportionate to the purposes  
5 listed in this section; and

6 (2) Adequate, relevant, and limited to what is necessary  
7 in relation to the specific purposes listed in this  
8 section. Personal data collected, used, or retained  
9 pursuant to subsection (b) where applicable, shall  
10 consider the nature and purpose or purposes of the  
11 collection, use, or retention. The data shall be  
12 subject to reasonable administrative, technical, and  
13 physical measures to protect the confidentiality,  
14 integrity, and accessibility of the personal data and  
15 to reduce reasonably foreseeable risks of harm to  
16 consumers relating to the collection, use, or  
17 retention of personal data.

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



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

5 **§ -9 Investigative authority; civil investigative**  
6 **demand.** (a) Whenever the department has reasonable cause to  
7 believe that any person has engaged in, is engaging in, or is  
8 about to engage in any violation of this chapter, the department  
9 may either require or permit the person to file with the  
10 department a statement in writing or otherwise, under oath, as  
11 to all facts and circumstances concerning the subject matter.  
12 The department may also require any other data and information  
13 as the department may deem relevant to the subject matter of an  
14 investigation of a possible violation of this chapter and may  
15 make such special and independent investigations as the  
16 department may deem necessary in connection with the matter.

17 (b) In connection with the investigation, the department  
18 may issue a civil investigative demand to witnesses by which the  
19 department may:

20 (1) Compel the attendance of the witnesses;



1           (2) Examine the witnesses under oath before the department  
2                   or a court of record;

3           (3) Subject to subsection (d), require the production of  
4                   any books or papers that the department deems relevant  
5                   or material to the inquiry; and

6           (4) Issue written interrogatories to be answered by the  
7                   witness served or, if the witness served is a  
8                   corporation, partnership, association, governmental  
9                   agency, or any person other than a natural person, by  
10                  any officer or agent, who shall furnish the  
11                  information as is available to the witness.

12           The investigative powers of this subsection shall not abate  
13           or terminate by reason of any action or proceeding brought by  
14           the department under this chapter.

15           (c) When documentary material is demanded by a civil  
16           investigative demand, the demand shall not:

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

20           (2) Require the disclosure of any documentary material  
21                  that would be privileged, or production of which for



1           any other reason would not be required by a subpoena  
2           duces tecum issued by a court of the State.

3           (d) Where the information requested pursuant to a civil  
4   investigative demand may be derived or ascertained from the  
5   business records of the party upon whom the interrogatory has  
6   been served or from an examination, audit, or inspection of the  
7   business records, or from a compilation, abstract, or summary  
8   based therein, and the burden of deriving or ascertaining the  
9   answer is substantially the same for the department as for the  
10   party from whom the information is requested, it shall be  
11   sufficient for that party to specify the records from which the  
12   answer may be derived or ascertained and to afford the  
13   department, or other individuals properly designated by the  
14   department, reasonable opportunity to examine, audit, or inspect  
15   the records and to make copies, compilations, abstracts, or  
16   summaries. Further, the department may elect to require the  
17   production pursuant to this section of documentary material  
18   before or after the taking of any testimony of the person  
19   summoned pursuant to a civil investigative demand, in which  
20   event, the documentary matter shall be made available for  
21   inspection and copying during normal business hours at the



1 principal place of business of the person served, or at any  
2 other time and place, as may be agreed upon by the person served  
3 and the department.

4 (e) Any civil investigative demand issued by the  
5 department shall contain the following information:

6 (1) The statute alleged to have been violated and the  
7 subject matter of the investigation;

8 (2) The date, place, time, and locations at which the  
9 person is required to appear to produce documentary  
10 material in the person's possession, custody, or  
11 control; provided that the date shall not be less than  
12 twenty days after the date of the civil investigative  
13 demand; and

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

17 (f) Service of civil investigative demand of the  
18 department may be made by:

19 (1) Delivery of a duly executed copy to the person served,  
20 or if a person is not a natural person, to the



1 principal place of business of the person to be  
2 served; or

3 (2) Mailing by certified mail, return receipt requested,  
4 of a duly executed copy addressed to the person to be  
5 served at the person's principal place of business in  
6 the State, or if the person has no place of business  
7 in the State, to the person's office.

8 (g) Within twenty days after the service of a demand upon  
9 any person or enterprise, or at any time before the return date  
10 specified in the demand, whichever period is shorter, the party  
11 may file in the circuit court and serve upon the attorney  
12 general a petition for an order modifying or setting aside the  
13 demand. The time allowed for compliance with the demand in  
14 whole or in part as deemed proper and ordered by the court shall  
15 not run during the pendency of the petition in the court. The  
16 petition shall specify each ground upon which the petitioner  
17 relies in seeking relief, and may be based upon any failure of  
18 the demand to comply with the provisions of this chapter or upon  
19 any constitutional or other legal right or privilege of the  
20 party. This subsection shall be the exclusive means for a  
21 witness summoned pursuant to a civil investigative demand





1 pursuant to this section to challenge the civil investigative  
2 demand.

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

9 (i) Any person required to testify or to submit  
10 documentary evidence shall be entitled, on payment of lawfully  
11 prescribed cost, to procure a copy of any document produced by  
12 the person and of the person's own testimony as stenographically  
13 reported or, in the case of depositions, as reduced to writing  
14 by or under the direction of a person taking the deposition.  
15 Any party compelled to testify or to produce documentary  
16 evidence may be accompanied and advised by counsel, but counsel  
17 may not, as a matter of right, otherwise participate in the  
18 investigation.

19 (j) Any persons served with a civil investigative demand  
20 by the department under this chapter, other than any person  
21 whose conduct or practices are being investigated or any



1 officer, director, or person in the employ of the person under  
2 investigation, shall be paid the same fees and mileage as paid  
3 witnesses in the courts of the State. No person shall be  
4 excused from attending an inquiry pursuant to the mandate of a  
5 civil investigative demand, or from producing a paper, or from  
6 being examined or required to answer questions on the ground of  
7 failure to tender or pay a witness fee or mileage unless demand  
8 is made at the time testimony is about to be taken and as a  
9 condition precedent to offering the production or testimony and  
10 unless payment is not made upon the demand.

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

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



1 civil investigative demand or lawful request by the department,  
2 pursuant to this 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 civil  
7 investigative demand or under order of the court on the ground  
8 that the testimony or evidence required of the person may tend  
9 to incriminate the person or subject the person to any penalty;  
10 provided that no testimony or other information compelled either  
11 by the department or under order of the court, or any  
12 information directly or indirectly derived from the testimony or  
13 other information, may be used against the individual or witness  
14 in any criminal case. A person may be prosecuted or subjected  
15 to penalty or forfeiture for any perjury, false swearing, or  
16 contempt committed in answering, or failing to answer, or in  
17 producing evidence or failing to do so in accordance with the  
18 order of the department or the court. If a person refuses to  
19 testify or produce evidence after being granted immunity from  
20 prosecution and after being ordered to testify or produce  
21 evidence, the person may be adjudged in contempt by a court of



1 pursuant to section 710-1077. This subsection shall not be  
2 construed to prevent the department from instituting other  
3 appropriate contempt proceedings against any person who violates  
4 this section.

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

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

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



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

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

Violation of this subsection shall be a misdemeanor.

**§ -10 Enforcement; civil penalty; expenses.** (a) The department shall have exclusive authority to enforce the provisions of this chapter.

(b) Before initiating any action under this chapter, the department shall provide a controller or processor a thirty-day written notice that identifies the specific provisions of this chapter that the controller or processor has allegedly violated. If, within the thirty-day period, the controller or processor cures the alleged violation and provides the department with an express written statement that the alleged violation has been cured and that no further violations shall occur, no action shall be initiated against the controller or processor.

(c) If a controller or processor continues to violate this chapter following the cure period in subsection (b) or breaches



1 the express written statement provided to the department  
2 pursuant to subsection (b), the department may:

- 3 (1) Initiate an action in the name of the State;
- 4 (2) Seek an injunction to restrain any violations of this  
5 chapter; and
- 6 (3) Seek to impose civil penalties of up to \$7,500 for  
7 each violation under this chapter.

8 (d) For any action initiated under this chapter, the  
9 department may recover reasonable expenses, including attorney  
10 fees, that the department incurred in the investigation and  
11 preparation of the case.

12 (e) Nothing in this chapter shall be construed as  
13 providing the basis for, or be subject to, a private right of  
14 action for violations of this chapter or under any other law.

15 **§ -11 Consumer privacy special fund.** (a) There is  
16 established in the state treasury the consumer privacy special  
17 fund into which shall be deposited:

- 18 (1) All civil penalties, expenses, and attorney fees  
19 collected pursuant to this chapter;
- 20 (2) Interest earned on money in the fund; and
- 21 (3) Appropriations made by the legislature.



1 (b) The fund shall be administered by the department.  
2 Moneys in the fund shall be used by the department to administer  
3 this chapter.

4 **§ -12 Rules.** The department shall adopt rules, pursuant  
5 to chapter 91, necessary for the purposes of this chapter."

6 SECTION 2. There is appropriated out of the general  
7 revenues of the State the sum of \$ or so much thereof  
8 as may be necessary for fiscal year 2022-2023 to be deposited  
9 into the consumer privacy special fund.

10 SECTION 3. There is appropriated out of the consumer  
11 privacy special fund the sum of \$ or so much thereof  
12 as may be necessary for fiscal year 2022-2023 for consumer data  
13 protection.

14 The sum appropriated shall be expended by the department of  
15 the attorney general for the purposes of this Act.

16 SECTION 4. This Act does not affect rights and duties that  
17 matured, penalties that were incurred, and proceedings that were  
18 begun before its effective date.

19 SECTION 5. This Act shall take effect on July 1, 2022.

20

INTRODUCED BY: 



# S.B. NO. 2797

**Report Title:**

Consumers; Data; Privacy; Attorney General; Appropriation

**Description:**

Establishes a framework to regulate controllers and processors with access to personal consumer data. Establishes penalties. Establishes a new consumer privacy special fund. Appropriates moneys.

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

