

1 (3) Power to exercise controlling influence over the
2 management of a company.

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

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

17 "Business associate" shall have the same meaning as in
18 title 45 Code of Federal Regulations section 160.103.

19 "Child" means any natural person younger than thirteen
20 years of age.



1 "Consent" means a clear affirmative act signifying a
2 consumer's freely given, specific, informed, and unambiguous
3 agreement to allow the processing of personal data relating to
4 the consumer. "Consent" includes a written statement, including
5 a statement written by electronic means, or any other
6 unambiguous affirmative action. "Consent" does not include:

- 7 (1) Acceptance of general or broad terms of use or
8 document containing general or broad descriptions of
9 personal data processing along with other unrelated
10 information;
- 11 (2) Hovering over, muting, pausing, or closing a given
12 piece of content; or
- 13 (3) Agreement obtained through the use of dark patterns.

14 "Consumer" means a natural person who is a resident of the
15 State acting only in an individual or household context.

16 "Consumer" does not include a natural person acting in a
17 commercial or employment context.

18 "Controller" means the natural or legal person that, alone
19 or jointly with others, determines the purpose and means of
20 processing personal data.



1 "Covered entity" shall have the same meaning as in title 45
2 Code of Federal Regulations section 160.103.

3 "Dark patterns" means a user interface designed or
4 manipulated with the substantial effect of subverting or
5 impairing user autonomy, decision-making, or choice. "Dark
6 patterns" includes any practice referred to by the Federal Trade
7 Commission as a "dark pattern".

8 "De-identified data" means data that cannot reasonably be
9 linked to an identified or identifiable natural person, or a
10 device linked to the person.

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

12 "Fund" means the consumer privacy special fund established
13 pursuant to section -12.

14 "Health Insurance Portability and Accountability Act" means
15 the Health Insurance Portability and Accountability Act of 1996,
16 P.L. 104-191, as amended.

17 "Identified or identifiable natural person" means a natural
18 person who may be readily identified, directly, or indirectly.

19 "Institution of higher education" means:

- 20 (1) The university of Hawaii system, or one of its
21 campuses; or



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

3 "Nonprofit organization" means any:

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

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

8 (3) Electric utility cooperative association subject to
9 chapter 421C.

10 "Personal data" means any information that is linked or
11 could be reasonably linkable to an identified or identifiable
12 natural person. "Personal data" does not include de-identified
13 data or publicly available information.

14 "Precise geolocation data" means information derived from
15 technology, including global positioning system level latitude
16 and longitude coordinates or other mechanisms, that directly
17 identifies the specific location of a natural person with
18 precision and accuracy within a radius of 1,750 feet. "Precise
19 geolocation data" does not include the content of communications
20 or any data generated by, or connected to, advanced utility



1 metering infrastructure systems or equipment for use by a
2 utility.

3 "Process" or "processing" means any operation or set of
4 operations performed, whether by manual or automated means, on
5 personal data or on sets of personal data, including the
6 collection, use, storage, disclosure, analysis, deletion, or
7 modification of personal data.

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

10 "Profiling" means any form of automated processing
11 performed on personal data to evaluate, analyze, or predict
12 personal aspects related to an identified or identifiable
13 natural person's economic situation, health, personal
14 preferences, interests, reliability, behavior, location, or
15 movements.

16 "Pseudonymous data" means personal data that cannot be
17 attributed to a specific natural person without the use of
18 additional information that is:

- 19 (1) Stored separately; and
20 (2) Subject to appropriate technical and organizational
21 measures to ensure that the personal data is not



1 attributed to an identified or identifiable
2 individual.

3 "Publicly available information" means information that is
4 lawfully made available through federal, state, or local
5 government records, or information that a business has a
6 reasonable basis to believe is lawfully made available to the
7 general public through widely distributed media, by the
8 consumer, or by a person to whom the consumer has disclosed the
9 information, unless the consumer has restricted the information
10 to a specific audience.

11 "Sale of personal data" means the exchange of personal data
12 for monetary or other valuable consideration by the controller
13 to a third party. "Sale of personal data" does not include:

14 (1) The disclosure of personal data to a processor that
15 processes the personal data on behalf of the
16 controller;

17 (2) The disclosure of personal data to a third party for
18 purposes of providing a product or service requested
19 by the consumer;

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



1 (4) The disclosure of personal data in which the consumer
2 directs the controller to disclose the personal data
3 or intentionally uses the controller to interact with
4 a third party;

5 (5) The disclosure of information that the consumer:

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

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

9 (6) The disclosure or transfer of personal data to a third
10 party as an asset that is part of an actual or
11 proposed merger, acquisition, bankruptcy, or other
12 transaction in which the third party assumes control
13 of all or part of the controller's assets.

14 "Sensitive data" means a category of personal data.

15 "Sensitive data" includes:

16 (1) Personal data revealing racial or ethnic origin,
17 religious beliefs, mental or physical health
18 conditions or diagnoses, sexual history, sexual
19 orientation, or citizenship or immigration status;

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



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

2 (4) Precise geolocation data.

3 "Targeted advertising" means displaying to a consumer
4 advertisements based on personal data obtained or inferred from
5 that consumer's activities over time and across non-affiliated
6 websites or online applications to predict the consumer's
7 preferences or interests. "Targeted advertising" does not
8 include:

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

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

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

16 (4) Processing personal data solely to measure or report
17 advertising performance, reach, or frequency.

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



1 **§ -2 Scope; exemptions.** (a) This chapter applies to
2 persons that conduct business in the State or produce products
3 or services that are targeted to residents of the State and
4 during a calendar year:

- 5 (1) Control or process personal data of at least one
6 hundred thousand consumers; or
7 (2) Control or process personal data of at least
8 twenty-five thousand consumers and derive over
9 twenty-five per cent of gross revenue from the sale of
10 personal data.

11 (b) This chapter shall not apply to:

- 12 (1) Any government entity;
13 (2) Any nonprofit organization;
14 (3) Any institution of higher education; or
15 (4) The National Insurance Crime Bureau.

16 (c) The following information and data are exempt from
17 this chapter:

- 18 (1) Protected health information as defined in title 45
19 Code of Federal Regulations section 160.103;
20 (2) Nonpublic personal information, as defined in the
21 Gramm-Leach-Bliley Act (15 U.S.C. chapter 94);



- 1 (3) Confidential records described in title 42 United
2 States Code section 290dd-2;
- 3 (4) Identifiable private information for purposes of the
4 protection of human subjects under title 45 Code of
5 Federal Regulations part 46; identifiable private
6 information that is otherwise collected as part of
7 human subjects research pursuant to the good clinical
8 practice guidelines issued by the International
9 Council for Harmonisation of Technical Requirements
10 for Pharmaceuticals for Human Use; identifiable
11 private information collected as part of a clinical
12 investigation under title 21 Code of Federal
13 Regulations parts 50 and 56; personal data used or
14 shared in research conducted in accordance with the
15 requirements set forth in this chapter; and other
16 research conducted in accordance with applicable law;
- 17 (5) Information and documents created for purposes of the
18 Health Care Quality Improvement Act of 1986 (42 U.S.C.
19 chapter 117);



- 1 (6) Patient safety work product for purposes of the
2 Patient Safety and Quality Improvement Act (42 U.S.C.
3 sections 299b-21 to 299b-26);
- 4 (7) Information derived from any of the health
5 care-related information listed in this subsection
6 that is de-identified in accordance with the
7 requirements for de-identification pursuant to the
8 Health Insurance Portability and Accountability Act;
- 9 (8) Information originating from, and intermingled so as
10 to be indistinguishable with, or information treated
11 in the same manner as information exempt under this
12 subsection that is maintained by a covered entity or
13 business associate as defined in the Health Insurance
14 Portability and Accountability Act or a program or a
15 qualified service organization as defined in title 42
16 Code of Federal Regulations section 2.11;
- 17 (9) Information used only for public health activities and
18 purposes as authorized by the Health Insurance
19 Portability and Accountability Act;
- 20 (10) The collection, maintenance, disclosure, sale,
21 communication, or use of any personal information



1 bearing on a consumer's credit worthiness, credit
2 standing, credit capacity, character, general
3 reputation, personal characteristics, or mode of
4 living by a consumer reporting agency or furnisher
5 that provides information for use in a consumer
6 report, and by a user of a consumer report, but only
7 to the extent that the activity is regulated by and
8 authorized under the Fair Credit Reporting Act
9 (15 U.S.C. sections 1681 to 1681x);

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

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

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

18 (14) Data processed or maintained:

19 (A) In the course of an individual applying to,
20 employed by, or acting as an agent or independent
21 contractor of a controller, processor, or third



1 party, to the extent that the data is collected
2 and used within the context of that role;

3 (B) As the emergency contact information of an
4 individual under this chapter used for emergency
5 contact purposes; or

6 (C) As necessary to retain to administer benefits for
7 another individual relating to the individual
8 under subparagraph (A) and used for the purposes
9 of administering those benefits.

10 (d) Controllers and processors that comply with the
11 verifiable parental consent requirements of the Children's
12 Online Privacy Protection Act (15 U.S.C. chapter 91) shall be
13 deemed compliant with any obligation to obtain parental consent
14 under this chapter.

15 **§ -3 Personal data rights; consumers.** (a) A consumer
16 may invoke the consumer rights specified in this subsection at
17 any time by submitting a request to a controller specifying the
18 consumer rights that the consumer wishes to invoke. A child's
19 parent or legal guardian may invoke the same consumer rights on
20 behalf of the child regarding processing personal data belonging



1 to the child. A controller shall comply with an authenticated
2 consumer request to exercise the right:

3 (1) To confirm whether or not a controller is processing
4 the consumer's personal data and to access the
5 personal data;

6 (2) To correct inaccuracies in the consumer's personal
7 data, taking into account the nature of the personal
8 data and the purposes of the processing of the
9 consumer's personal data;

10 (3) To delete personal data provided by the consumer;

11 (4) To obtain a copy of the consumer's personal data that
12 the consumer previously provided to the controller in
13 a format that:

14 (A) Is portable;

15 (B) To the extent technically feasible, is readily
16 usable; and

17 (C) If the processing is carried out by automated
18 means, allows the consumer to transmit the data
19 to another controller without hindrance; and

20 (5) To opt-out of the processing of the personal data for
21 purposes of:



1 (A) Targeted advertising;
2 (B) The sale of personal data; or
3 (C) Profiling in furtherance of decisions made by the
4 controller that results in the provision or
5 denial by the controller of financial and lending
6 services; housing; insurance; education
7 enrollment; criminal justice; employment
8 opportunities; health care services; or access to
9 basic necessities, including food and water.

10 (b) A consumer may exercise rights under this section by
11 secure and reliable means established by the controller and
12 described to the consumer in the controller's privacy notice. A
13 consumer may designate an authorized agent in accordance with
14 section -4 to exercise the rights of the consumer to opt-out
15 of the processing of the consumer's personal data for purposes
16 of subsection (a)(5) on behalf of the consumer. In the case of
17 processing personal data of a known child, the parent or legal
18 guardian of the child may exercise the child's consumer rights
19 on the child's behalf. In the case of processing personal data
20 concerning a consumer subject to a guardianship,
21 conservatorship, or other protective arrangement, the guardian



1 or conservator of the consumer may exercise the consumer's
2 rights on the consumer's behalf.

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

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



1 take action and instructions for appealing the
2 decision pursuant to subsection (d);

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

13 (4) If a controller is unable to authenticate the request
14 using commercially reasonable efforts, the controller
15 shall not be required to comply with a request to
16 initiate an action under subsection (a) and may
17 request that the consumer provide additional
18 information reasonably necessary to authenticate the
19 consumer and the consumer's request; provided that no
20 controller shall be required to authenticate an
21 opt-out request; provided further that a controller



1 may deny an opt-out request if the controller has a
2 good faith, reasonable, and documented belief that the
3 request is fraudulent; provided further that if a
4 controller denies an opt-out request because the
5 controller believes that the request is fraudulent,
6 the controller shall send a notice to the person who
7 made the request disclosing that the controller
8 believes the request is fraudulent, why the controller
9 believes the request is fraudulent, and that the
10 controller shall not comply with the request; and

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

16 (A) Retaining a record of the deletion request and
17 the minimum data necessary for the purpose of
18 ensuring the consumer's personal data remains
19 deleted from the business's records and not using
20 the retained data for any other purpose pursuant
21 to the provisions of this chapter; or



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

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

18 **§ -4 Authorized agent; designation; powers.** A consumer
19 may designate another person to serve as the consumer's
20 authorized agent, act on the consumer's behalf, or opt-out of
21 the processing of the consumer's personal data for one or more



1 of the purposes specified in section -3(a)(5). The consumer
2 may designate an authorized agent by way of, among other things,
3 a computer technology, including an internet link, browser
4 setting, browser extension, or global device setting, indicating
5 the consumer's intent to opt-out of the processing. A
6 controller shall comply with an opt-out request received from an
7 authorized agent if the controller is able to verify, with
8 commercially reasonable effort, the identity of the consumer and
9 the authorized agent's authority to act on the consumer's
10 behalf.

11 **§ -5 Controller responsibilities; transparency. (a)**

12 Each controller shall:

- 13 (1) Limit the collection of personal data to data that is
14 adequate, relevant, and reasonably necessary in
15 relation to the purposes for which the data is
16 processed, as disclosed to the consumer;
- 17 (2) Except as otherwise provided in this chapter, not
18 process personal data for purposes that are neither
19 reasonably necessary to, nor compatible with, the
20 disclosed purposes for which the personal data is



- 1 processed, as disclosed to the consumer, unless the
2 controller obtains the consumer's consent;
- 3 (3) Establish, implement, and maintain reasonable
4 administrative, technical, and physical data security
5 practices to protect any confidential information
6 contained in, and the integrity and accessibility of,
7 personal data. The data security practices shall be
8 appropriate to the volume and nature of the personal
9 data at issue;
- 10 (4) Provide an effective mechanism for a consumer to
11 revoke the consumer's consent under this section that
12 is at least as easy to use as the mechanism by which
13 the consumer provided the consumer's consent and, upon
14 revocation of the consumer's consent, cease to process
15 the data as soon as practicable, but not later than
16 fifteen days after the receipt of the request;
- 17 (5) Not process the personal data of a consumer for
18 purposes of targeted advertising, or sell the
19 consumer's personal data without the consumer's
20 consent, under circumstances in which the controller
21 has actual knowledge, and willfully disregards, that



1 the consumer is at least thirteen years of age but
2 younger than sixteen years of age; provided that no
3 controller shall discriminate against a consumer for
4 exercising any of the consumer rights contained in
5 this chapter, including denying goods or services,
6 charging different prices or rates for goods or
7 services, or providing a different level of quality of
8 goods or services to the consumer;

9 (6) Not process personal data in violation of state and
10 federal laws that prohibit unlawful discrimination
11 against consumers; and

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

18 provided that nothing in this subsection shall be construed to
19 require a controller to provide a product or service that
20 requires the personal data of a consumer that the controller
21 does not collect or maintain, or prohibit a controller from



1 offering a different price, rate, level, quality, or selection
2 of goods or services to a consumer, including offering goods or
3 services for no fee, if the offering is in connection with a
4 consumer's voluntary participation in a bona fide loyalty,
5 rewards, premium features, discounts, or club card program.

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

10 (c) Each controller shall provide to each applicable
11 consumer a reasonably accessible, clear, and meaningful privacy
12 notice that includes:

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



1 (5) The categories of third parties, if any, with whom the
2 controller shares personal data; and

3 (6) An active electronic mail address or other online
4 mechanism that the consumer may use to contact the
5 controller.

6 (d) If a controller sells personal data to third parties
7 or processes personal data for targeted advertising, the
8 controller shall clearly and conspicuously disclose to the
9 affected consumer the processing and manner in which the
10 consumer may exercise the right to opt-out of the processing.

11 (e) A controller shall establish, and shall describe in a
12 privacy notice, one or more secure and reliable means for each
13 consumer to submit a request to exercise the consumer's rights
14 under this chapter. These means shall take into account the
15 ways in which consumers normally interact with the controller,
16 the need for secure and reliable communication of the requests,
17 and the ability of the controller to authenticate the identity
18 of the consumer making the request. No controller shall require
19 a consumer to create a new account in order to exercise the
20 consumer's rights pursuant to section -3, but may require a
21 consumer to use an existing, active account.



1 (f) No controller shall discriminate against a consumer
2 for exercising any of the consumer rights contained in this
3 chapter, including denying goods or services, charging different
4 prices or rates for goods or services, or providing a different
5 level of quality of goods and services to the consumer; provided
6 that nothing in this chapter shall be construed to require a
7 controller to:

8 (1) Provide a product or service that requires the
9 personal data of a consumer that the controller does
10 not collect or maintain; or

11 (2) Prohibit a controller from offering a different price,
12 rate, level, quality, or selection of goods or
13 services to a consumer, including offering goods or
14 services for no fee, if:

15 (A) The consumer has exercised the consumer's right
16 to opt-out pursuant to section -3; or

17 (B) The offer is related to a consumer's voluntary
18 participation in a bona fide loyalty, rewards,
19 premium features, discounts, or club card
20 program.



1 **§ -6 Responsibility according to role; controller and**
2 **processor.** (a) In meeting its obligations under this chapter,
3 each processor shall adhere to the instructions of a controller
4 and 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 is
8 reasonably practicable, to fulfill the controller's
9 obligation to respond to consumer rights requests

10 pursuant to section -3;

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

17 (3) The provision of necessary information to enable the
18 controller to conduct and document data protection
19 assessments pursuant to section -7.

20 (b) A contract between a controller and a processor shall
21 govern the processor's data processing procedures with respect



1 to processing performed on behalf of the controller. The
2 contract shall be binding and clearly set forth instructions for
3 processing, the nature and purpose of processing, the type of
4 data subject to processing, the duration of processing, and the
5 rights and obligations of both parties. The contract shall also
6 include requirements that the processor shall:

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

10 (2) At the controller's direction, delete or return all
11 personal data to the controller upon request at the
12 end of the provision of services, unless retention of
13 the personal data is required by law;

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

19 (4) Allow, and cooperate with, any reasonable assessments
20 of the processor's policies and technical and
21 organizational measures in support of the processor's



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

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

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

18 (d) A determination of whether a person is acting as a
19 controller or processor with respect to a specific processing of
20 data is a fact-based determination that depends upon the context
21 in which personal data is to be processed. A person who is not



1 limited in the processing of personal data pursuant to a
2 controller's instructions, or who fails to adhere to these
3 instructions, shall be deemed to be a controller and not a
4 processor with respect to the specific processing of data. A
5 processor that continues to adhere to a controller's
6 instructions with respect to a specific processing of personal
7 data shall remain a processor. If a processor begins, alone or
8 jointly with others, determining the purposes and means of the
9 processing of personal data, the processor shall be deemed to be
10 a controller.

11 **§ -7 Data protection assessments.** (a) The data
12 protection assessment requirements of this section shall apply
13 to processing activities created or generated after January 1,
14 2025.

15 (b) Each controller shall conduct and document a data
16 protection assessment of each of the following processing
17 activities involving personal data:

- 18 (1) The processing of personal data for purposes of
19 targeted advertising;
- 20 (2) The sale of personal data;



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



1 controller to reduce these risks. The controller shall factor
2 into this assessment the use of de-identified data, the
3 reasonable expectations of consumers, the context of the
4 processing, and the relationship between the controller and the
5 consumer whose personal data is processed.

6 (d) The department may request, pursuant to a civil
7 investigative demand, that a controller disclose any data
8 protection assessment that is relevant to an investigation
9 conducted by the department, and the controller shall make the
10 data protection assessment available to the department. The
11 department may evaluate the data protection assessment for
12 compliance with the responsibilities set forth in section -5.
13 Data protection assessments shall be confidential and exempt
14 from the public inspection and copying requirements of chapter
15 92F. The disclosure of a data protection assessment pursuant to
16 a request from the department shall not constitute a waiver of
17 attorney-client privilege or work product protection with
18 respect to the assessment and any information contained in the
19 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 **§ -8 Processing de-identified data; exemptions.** (a) A
9 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 technological
3 information, in order to be capable of associating an
4 authenticated 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 received pursuant to section -3 if:

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

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

17 (3) The controller does not sell the personal data to any
18 third party or otherwise voluntarily disclose the
19 personal data to any third party other than a
20 processor, except as otherwise permitted in this
21 section.



1 (d) The consumer rights specified in sections -3(a)(1)
2 to (4) and section -5 shall not apply to pseudonymous data in
3 cases in which the controller is able to demonstrate that any
4 additional information necessary to identify the consumer is
5 kept separately and is subject to effective technical and
6 organizational controls that:

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

9 (2) Prevent the controller from 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 **§ -9 Limitations.** (a) Nothing in this chapter shall be
17 construed to restrict a controller 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 if 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 these 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 whether:
- 10 (A) 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) The controller has implemented reasonable
16 safeguards to mitigate privacy risks associated
17 with research, including any risks associated
18 with reidentification;
- 19 (9) Assist another controller, processor, or third party
20 with any of the obligations under this subsection; or



1 (10) Process personal data for reasons of public interest
2 in the area of public health, community health, or
3 population health, but only to the extent that
4 processing is:

5 (A) Subject to suitable and specific measures to
6 safeguard the rights of the consumer whose
7 personal data is being processed; and

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

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

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

16 (2) Effectuate a product recall;

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

19 (4) Perform internal operations that are reasonably
20 aligned with the expectations of the consumer,
21 reasonably anticipated based on the consumer's



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

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

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



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

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

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

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

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



1 pursuant to this section may be processed to the extent that the
2 processing is:

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

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

18 (g) If a controller processes personal data pursuant to an
19 exemption in this section, the controller shall bear the burden
20 of 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 **§ -10 Investigative authority.** The department may
6 investigate alleged violations of this chapter pursuant to
7 section 28-2.5 and any other applicable law.

8 **§ -11 Enforcement; civil penalty; expenses.** (a) The
9 department shall have exclusive authority to enforce this
10 chapter.

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

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



1 or breaches the express written statement provided to the
2 department 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 to provide
13 the basis for, or be subject to, a private right of action for
14 violations of this chapter or under any other law.

15 **§ -12 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 moneys 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 **§ -13 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 2023-2024 and the same sum
9 or so much thereof as may be necessary for fiscal year 2024-2025
10 to be deposited into the consumer privacy special fund.

11 SECTION 3. There is appropriated out of the consumer
12 privacy special fund the sum of \$ or so much thereof
13 as may be necessary for fiscal year 2023-2024 and the same sum
14 or so much thereof as may be necessary for fiscal year 2024-2025
15 for consumer data protection.

16 The sums appropriated shall be expended by the department
17 of the attorney general for the purposes of this Act.

18 SECTION 4. 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.

21 SECTION 5. This Act shall take effect on July 1, 2050.



Report Title:

Consumers; Data; Privacy; Attorney General; Appropriations

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. Effective 7/1/2050. (SD2)

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

