34-LS1485\G
Walsh
4/15/26

CS FOR HOUSE BILL NO. 367(JUD)

IN THE LEGISLATURE OF THE STATE OF ALASKA

THIRTY-FOURTH LEGISLATURE - SECOND SESSION

BY THE HOUSE JUDICIARY COMMITTEE

Offered:
Referred:

Sponsor(s): REPRESENTATIVE STORY

A BILL

FOR AN ACT ENTITLED

"An Act relating to the privacy of consumer personal data; establishing data broker registration requirements; relating to social security numbers; making certain violations unfair or deceptive trade practices; and providing for an effective date."

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

*** Section 1.** AS 37.05.146(c) is amended by adding a new paragraph to read:

(87) consumer privacy account (AS 45.48.860).

*** Sec. 2.** AS 44.33.020(a) is amended by adding a new paragraph to read:

(45) establish and maintain a data broker registry under AS 45.48.855.

*** Sec. 3.** AS 45.48.430(b) is amended to read:

(b) The prohibition in (a) of this section does not apply if

(1) the disclosure is authorized by local, state, or federal law, including **AS 45.48.800 - 45.48.898 or** a regulation adopted under AS 45.48.470;

(2) the person is engaging in the business of government and

(A) is authorized by law to disclose the individual's social

security number; or

(B) the disclosure of the individual's social security number is required for the performance of the person's duties or responsibilities as provided by law;

(3) the disclosure is to a person subject to or for a transaction regulated by the Gramm-Leach-Bliley Financial Modernization Act, and the disclosure is for a purpose authorized by the Gramm-Leach-Bliley Financial Modernization Act or to facilitate a transaction of the individual;

(4) the disclosure is to a person subject to or for a transaction regulated by the Fair Credit Reporting Act, and the disclosure is for a purpose authorized by the Fair Credit Reporting Act;

(5) the disclosure is part of a report prepared by a consumer credit reporting agency in response to a request by a person and the person submits the social security number as part of the request to the consumer credit reporting agency for the preparation of the report; or

(6) the disclosure is for a background check on the individual, identity verification, fraud prevention, medical treatment, law enforcement or other government purposes, or the individual's employment, including employment benefits.

*** Sec. 4.** AS 45.48.450(b) is amended to read:

(b) Notwithstanding the other provisions of AS 45.48.400 - 45.48.480, and except as provided **under AS 45.48.800 - 45.48.898 or** for an agent under (a) of this section, a person may disclose an individual's social security number to an independent contractor of the person to facilitate the purpose or transaction for which the individual initially provided the social security number to the person, but the independent contractor may not use the social security number for another purpose or make an unauthorized disclosure of the individual's personal information. In this subsection, "independent contractor" includes a debt collector.

*** Sec. 5.** AS 45.48 is amended by adding new sections to read:

Article 6A. Data Privacy.

Sec. 45.48.800. Applicability. (a) AS 45.48.800 - 45.48.898 apply to a person that conducts business in the state or produces products or provides services targeted

to residents of this state and that, during the preceding calendar year, collected or processed the personal data of at least

(1) 35,000 consumers, not including personal data controlled or processed solely for the purpose of completing a payment transaction; or

(2) 10,000 consumers and derived more than 20 percent of the person's gross revenue from the sale of personal data.

(b) AS 45.48.800 - 45.48.898 do not apply to the federal government, the state, a public corporation of the state, the University of Alaska, a municipality, a school district, a regional educational attendance area, or a tribal government.

Sec. 45.48.805. Consumer rights. (a) A consumer has the right to

(1) confirm whether a controller is collecting or processing the consumer's personal data and access that personal data;

(2) obtain from a controller a list of specific third parties, other than natural persons, to which the controller has transferred either

(A) the consumer's personal data; or

(B) any personal data;

(3) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

(4) delete personal data provided by, or obtained about, the consumer, including personal data the consumer provided to the controller, personal data the controller obtained from another source, and data derived from the personal data;

(5) obtain a copy of the consumer's personal data collected or processed by the controller, in a portable and, to the extent technically practicable, readily usable format that allows the consumer to transmit the data to another controller without hindrance if the processing is carried out by automated means; and

(6) opt out of the collection and processing of the consumer's personal data for purposes of

(A) targeted advertising;

(B) the sale of personal data; or

(C) profiling in furtherance of automated decisions that

produce legal or similarly significant effects concerning the consumer.

(b) A parent or legal guardian of a minor may exercise the minor's consumer rights under this section on the minor's behalf. A guardian or conservator of a consumer subject to a guardianship, conservatorship, or other protective arrangement may exercise the consumer's rights under this section on the consumer's behalf.

(c) A consumer may designate another person to serve as the consumer's authorized agent, and act on the consumer's behalf, to exercise the consumer's rights under this section. A controller shall comply with a request from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the agent's authority to act on the consumer's behalf.

(d) A controller or processor may not collect, process, or transfer personal data in a manner that discriminates against an individual or class of individuals, or otherwise makes unavailable the equal enjoyment of goods or services, based on an individual's or class of individuals' actual or perceived race, color, sex, sexual orientation, gender identity, disability, religion, ancestry, or national origin. This subsection does not apply to

(1) the collection, processing, or transfer of personal data for the sole purpose of

(A) self-testing by a controller or processor to prevent or mitigate unlawful discrimination or otherwise to ensure compliance with state or federal law; or

(B) diversifying an applicant, participant, or customer pool; or

(2) a private establishment as described in 42 U.S.C. 2000a(e).

Sec. 45.48.810. Controller responses to consumer requests. (a) A consumer may exercise a consumer right under AS 45.48.805 by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. The means established by the controller must take into account the ways that a consumer normally interacts with the controller, the need for secure and reliable communication of a consumer request, and the ability of the controller to verify the identity of the consumer making the request. A controller may not require a consumer to create a new account to exercise a consumer right, but may require a consumer to

use an existing account.

(b) In addition to other means established by the controller, a controller shall allow a consumer to exercise an opt-out request under AS 45.48.805(a)(6) by providing

(1) a clear and conspicuous "Do Not Sell My Personal Information" or similarly worded link on the home page of the controller's Internet website; and

(2) an opt-out preference signal sent to the controller, with the consumer's consent, by a platform, technology, or mechanism used by the consumer that is consumer-friendly and easy for the average consumer to use and that allows the controller to reasonably determine whether the consumer is a resident of the state and whether the consumer has made a legitimate opt-out request; the use of an Internet protocol address to estimate the consumer's location is sufficient to reasonably determine residency under this paragraph.

(c) If a consumer's opt-out request under (b)(1) or (2) of this section conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's financial incentive program offered under AS 45.48.840, the controller shall comply with the consumer's opt-out preference provided under (b)(1) or (2) of this section but may notify the consumer of the conflict and provide to the consumer the choice to confirm the controller-specific privacy setting or participation in the program. If a controller responds to a consumer opt-out request under (b)(1) or (2) of this section by informing the consumer of a change in the price, rate, level, quality, or selection of goods or services, the controller shall present the terms of any financial incentive offered under AS 45.48.840 for the retention, processing, sale, or transfer of the consumer's personal data.

(d) Except as otherwise provided in AS 45.48.800 - 45.48.898, a controller shall comply with a request by a consumer to exercise the consumer's rights as follows:

(1) a controller shall respond to the consumer without undue delay, but not later than 45 days after receiving the request; the controller may extend the response period by 45 additional days when reasonably necessary, considering the complexity and number of the consumer's requests, if the controller informs the

consumer of the extension and the reason for the extension within the initial 45-day response period;

(2) if a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receiving the request, of the justification for declining to take action and provide instructions for how to appeal the decision;

(3) a controller shall provide information in response to a consumer request free of charge once for each consumer during any 12-month period; if a request from a consumer is manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request; the controller bears the burden of demonstrating that the request is manifestly unfounded, excessive, or repetitive;

(4) if a controller is unable to authenticate a request to exercise a right afforded by AS 45.48.805(a)(1) - (5) using commercially reasonable efforts, the controller is not required to comply with a request to initiate an action under this section and shall provide notice to the consumer that the controller is unable to authenticate the request until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request;

(5) a controller may not require a consumer to authenticate to exercise an opt-out request under AS 45.48.805(a)(6), but a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that the request is fraudulent; if a controller denies an opt-out request because the controller believes the request is fraudulent, the controller shall send a notice to the person who made the request disclosing that the controller believes the request is fraudulent, why the controller believes the request is fraudulent, and that the controller will not comply with the request;

(6) a controller that has obtained a consumer's personal data from a source other than the consumer complies with a consumer's request to delete the data under AS 45.48.805(a)(4) if the controller

(A) deletes the consumer's personal data retained by the

controller;

(B) retains a record of the deletion request and the minimum data necessary to ensure the consumer's personal data remains deleted from the controller's records; and

(C) does not use retained data for any other purpose.

(e) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period after the consumer receives the decision refusing to take action. The appeal process must be conspicuously available and similar to the process for the consumer to submit requests under this section. Not later than 60 days after receiving an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall provide the consumer with an online mechanism, if available, or another method by which the consumer may contact the attorney general to submit a complaint.

(f) A controller may not condition, expressly or effectively, or attempt to condition the exercise of a consumer right under this section through the use of

(1) a false, fictitious, fraudulent, or materially misleading statement or representation; or

(2) a dark pattern.

(g) A controller or processor is not required to comply with an authenticated consumer rights request if the controller or processor

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

(2) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer.

Sec. 45.48.815. Data minimization rules and de-identified data. (a) A controller shall limit the collection, processing, and transfer of personal data to that which is reasonably necessary to provide or maintain

(1) a specific product or service requested by the consumer to whom the data pertains and related routine administrative, operational, or account-servicing activity, including billing, shipping, delivery, storage, or accounting; and

(2) a communication, other than an advertisement, by the controller to the consumer reasonably anticipated within the context of the relationship between the controller and the consumer.

(b) A controller may process or transfer personal data collected under (a) of this section to provide first-party advertising or targeted advertising, except when otherwise prohibited under AS 45.48.800 - 45.48.898.

(c) A controller that possesses de-identified data shall

(1) take technical measures to ensure that the data cannot be associated with an individual;

(2) publicly commit to maintaining and using de-identified data without attempting to reidentify the data; and

(3) contractually obligate a recipient of the de-identified data to comply with the provisions of AS 45.48.800 - 45.48.898.

(d) A controller that transfers de-identified data shall exercise reasonable oversight to monitor compliance with contractual commitments to which the de-identified data is subject and shall take appropriate steps to address a breach of those contractual commitments.

(e) A controller or processor is not required to

(1) reidentify de-identified data; or

(2) maintain data in an identifiable form.

Sec. 45.48.820. Sensitive data. (a) A controller may not collect, process, or transfer sensitive data pertaining to a consumer unless the collection, processing, or transfer is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the sensitive data pertains.

(b) A controller may not sell sensitive data.

(c) A controller may not transfer sensitive data pertaining to a consumer without first obtaining the consumer's affirmative consent. A controller shall provide an effective mechanism for a consumer to revoke the consumer's affirmative consent

that is at least as easy as the mechanism the consumer used to provide the consumer's affirmative consent and, on revocation of the consumer's affirmative consent, the controller shall discontinue processing the data as soon as practicable, but not later than 15 days after receiving the consumer's revocation of affirmative consent.

(d) Notwithstanding any other provision of AS 45.48.800 - 45.48.898, a controller that knows or reasonably should know that a consumer is a minor may not

(1) process or transfer personal data of the minor for targeted advertising; or

(2) sell the personal data of the minor.

Sec. 45.48.825. Privacy notice and disclosures. (a) A controller shall provide a consumer with a reasonably accessible, clear, and meaningful privacy notice. The privacy notice must include

(1) the categories of personal data collected and processed by the controller and a separate list of categories of sensitive data collected and processed by the controller, described in a level of detail that provides the consumer a meaningful understanding of the type of personal data collected or processed;

(2) the purpose of collecting and processing each category of personal data the controller collects or processes, described in a way that gives the consumer a meaningful understanding of how each category of personal data will be used;

(3) how a consumer may exercise the consumer's rights under AS 45.48.800 - 45.48.898, including how a consumer may appeal a controller's decision about the consumer's request;

(4) the categories of personal data that the controller transfers to a third party, if applicable, and the purpose of that transfer;

(5) the categories of third parties, if any, to which the controller transfers personal data;

(6) the length of time the controller intends to retain each category of personal data or, if it is not possible to identify the length of time, the criteria used to determine the length of time the controller intends to retain each category of personal data; and

(7) an active electronic mail address or other online mechanism that

the consumer may use to contact the controller.

(b) If a controller makes a material change to the controller's privacy notice, the controller shall, before implementing the material change for prospectively collected personal data, notify each consumer affected by the material change and provide a reasonable opportunity for each consumer to withdraw consent. A controller shall provide a reasonable opportunity for each consumer to provide affirmative consent to further materially different processing or transfer of previously collected personal data under the changed policy. The controller shall take all reasonable measures to provide to each affected consumer direct electronic notification about material changes to the privacy notice, taking into account available technology and the nature of the relationship.

(c) If a controller sells personal data to a third party or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose that sale or processing, as well as the manner in which a consumer may exercise the right to opt out of that sale or processing.

Sec. 45.48.830. Responsibilities of processors and controllers. (a) A processor shall adhere to the instructions of a controller and assist the controller in meeting the controller's obligations under AS 45.48.800 - 45.48.898, taking into account the nature of the processing and the information available to the processor, including by

(1) using appropriate technical and organizational measures, to the extent reasonably practicable, to fulfill the controller's obligation to respond to a consumer rights request;

(2) assisting the controller in meeting the controller's obligations relating to the security of processing personal data and notification of a breach of security of the system of the processor to meet the controller's obligations; and

(3) providing necessary information to enable the controller to conduct and document a data protection assessment.

(b) A controller and a processor shall enter into a contract to govern the processor's data processing procedures for processing performed on behalf of the controller. The contract must be binding and clearly set out instructions for processing

data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The processor shall adhere to the instructions of the controller and process and transfer the data the processor receives from the controller only to the extent necessary to provide a service requested by the controller, as set out in the contract. The contract must also require that the processor

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

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

(3) at the reasonable request of the controller, make available to the controller information in the processor's possession that is necessary to demonstrate the processor's compliance with the obligations set out in AS 45.48.800 - 45.48.898;

(4) after providing the controller with an opportunity to object, engage a subcontractor under a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data if the processor engages a subcontractor;

(5) ensure that personal data that the processor receives from or on behalf of a controller not be combined with personal data that the processor receives from or on behalf of another person or collects from the interaction of the processor with an individual; and

(6) allow and cooperate with a reasonable assessment by the controller or the controller's designated assessor, or arrange for a qualified and independent assessor to conduct an assessment, of the processor's policies and technical and organizational measures in support of the obligations under AS 45.48.800 - 45.48.898, using an appropriate and accepted control standard or framework and assessment procedure, and provide a report of the assessment to the controller on request.

(c) Nothing in this section relieves a controller or processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship as described in AS 45.48.800 - 45.48.898.

(d) Whether a person is acting as a controller or processor with respect to a specific processing of personal data depends on the facts and the context in which the personal data is processed. A person who is not limited in the person's processing of personal data under a controller's instructions, or who fails to adhere to those instructions, is a controller and not a processor with respect to that specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor becomes a controller with respect to that processing.

Sec. 45.48.835. Data protection assessments. (a) Before initiating the processing activity, a controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer, including

(1) the collection or processing of personal data for the purpose of targeted advertising;

(2) the sale of personal data;

(3) the processing of personal data for the purpose of profiling, when the profiling presents a reasonably foreseeable risk of

(A) unfair or deceptive treatment of, or having an unlawfully disparate effect on, consumers;

(B) financial, physical, or reputational injury to consumers;

(C) a physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, when the intrusion would be offensive to a reasonable person; or

(D) other substantial injury to consumers; and

(4) the collection or processing of sensitive data.

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

(c) A data protection assessment conducted under this section must

(1) identify the categories of personal data collected, the purposes of collecting the personal data, and whether personal data is being transferred;

(2) consider the use of de-identified data, the reasonable expectations of consumers, the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed; and

(3) identify and weigh the benefits resulting, directly or indirectly, from the processing activity to the controller, the consumer, other stakeholders, and the public against the potential risks to the consumer's rights, as mitigated by safeguards that are employed by the controller to reduce those risks.

(d) Not later than 30 days after completing a data protection assessment under this section, a controller shall submit a report of the data protection assessment or evaluation to the attorney general. The report must include a summary of the data protection assessment. The controller shall make the summary publicly available on the controller's Internet website or another place that is easily accessible to consumers. A controller may redact confidential or proprietary information from the report. The attorney general may require a controller to disclose a data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller shall make the data protection assessment available to the attorney general. The attorney general may evaluate the data protection assessment for compliance with the controller's responsibilities under AS 45.48.800 - 45.48.898. To the extent information contained in a data protection assessment disclosed to the attorney general includes information subject to attorney-client privilege or protection under the work product doctrine, the disclosure does not constitute a waiver of the privilege or protection.

(e) A data protection assessment conducted by a controller for the purpose of complying with another applicable law satisfies the requirements in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise have been conducted under this section.

(f) A controller shall review and update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of personal data collected or processed and level of risk presented by the processing, throughout the duration of the processing activity,

(1) to monitor for harm caused by the processing and adjust safeguards accordingly; and

(2) to ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing.

Sec. 45.48.840. Discrimination, retaliation, and financial incentives. (a) A controller may not discriminate or retaliate against a consumer for exercising a consumer right under AS 45.48.800 - 45.48.898 or refusing to agree to the collection or processing of personal data for a separate product or service, including by

(1) denying goods or services;

(2) charging different prices or rates for goods or services;

(3) providing a different level of quality of goods or services to a consumer.

(b) A controller is not required to provide a product or service that requires a consumer's personal data that the controller does not collect or maintain.

(c) Notwithstanding (a) of this section, a controller may offer to a consumer a different price, rate, level, quality, or selection of goods or services, including goods or services for no fee, if the offer is made in connection with a consumer's voluntary participation in a financial incentive program, such as a bona fide loyalty, rewards, premium features, discount, or club card program. A controller that offers a financial incentive program under this subsection may not

(1) transfer personal data to a third party as part of the program unless

(A) the transfer is functionally necessary to enable the third party to provide a benefit to which the consumer is entitled;

(B) the transfer of personal data to the third party is clearly disclosed in the terms of the program; and

(C) the third party uses the personal data only for purposes of facilitating a benefit to which the consumer is entitled and does not process or transfer the personal data for any other purpose;

(2) consider the sale of personal data as functionally necessary to provide the program;

(3) use financial incentive practices that are unjust, unreasonable, coercive, or usurious.

Sec. 45.48.845. Transfer of information in a business change transaction.

(a) A controller may transfer to or share with a third party a consumer's personal data as an asset that is part of a business change transaction if, within a reasonable time before sharing or transferring the personal data, the controller provides an affected consumer with

(1) a notice describing the business change transaction, including the name of the third party receiving the consumer's personal data and the applicable privacy policies of the third party; and

(2) a reasonable opportunity to

(A) withdraw the previously provided consent related to the consumer's personal data; and

(B) request the deletion of the consumer's personal data.

(b) If a controller shares a consumer's personal data with a third party in the process of evaluating and consummating a business change transaction, the controller shall require that the third party agree by contract to keep the personal data confidential and not use the personal data for a purpose other than evaluating and consummating the transaction.

(c) A third party under (a) of this section may not use or share the consumer's personal data in a manner that is materially inconsistent with (a) of this section or with the privacy policy of the third party provided to the consumer in the notification required under (a) of this section.

(d) A transfer under (a) of this section does not authorize a controller to make material retroactive privacy policy changes or other changes in a manner that constitutes an unfair or deceptive trade practice under AS 45.50.471 - 45.50.561.

(e) In this section, "business change transaction" means a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of some or all of the controller's assets.

Sec. 45.48.850. Security procedures and practices. (a) A controller shall implement and maintain reasonable administrative, technical, and physical security procedures and practices to protect the confidentiality, integrity, and accessibility of personal data that are appropriate to the volume and nature of the data. The security procedures and practices adopted by a controller must include a retention schedule that

requires the deletion of personal data when the data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected, processed, or transferred.

(b) A processor shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

Sec. 45.48.855. Data broker registration. (a) Before a controller begins operating as a data broker, the controller shall register with the commissioner in accordance with this section.

(b) To register as a data broker, a controller shall

(1) provide, on a form provided by the commissioner,

(A) the name of the data broker;

(B) the data broker's primary physical and mailing addresses;

(C) the data broker's electronic mail address;

(D) the data broker's primary Internet website address; and

(E) the Internet website address for the data broker's "Do Not Sell My Personal Information" Internet website page as required under AS 45.48.810(b); and

(2) pay a registration fee in an amount established by the department by regulation.

(c) The department shall deposit the fees paid under this section into the consumer privacy account established under AS 45.48.860.

(d) The commissioner shall make available on the department's Internet website a registry with the information provided by data brokers under this section.

Sec. 45.48.860. Consumer privacy account. (a) The consumer privacy account is established in the general fund. Registration fees collected under AS 45.48.855 and civil penalties and money collected in or as a result of an action brought by the attorney general under AS 45.48.800 - 45.48.898 shall be deposited into the general fund and separately accounted for under AS 37.05.142.

(b) The legislature may appropriate the annual estimated balance in the

account maintained under AS 37.05.142 to pay

(1) the salaries of attorneys in the Department of Law that enforce the provisions of AS 45.48.800 - 45.48.898 at an amount that is competitive with the private sector; and

(2) the administrative costs incurred by the department and the Department of Law to enforce AS 45.48.800 - 45.48.898.

Sec. 45.48.865. Violations. (a) A violation of AS 45.48.800 - 45.48.898 is an unfair or deceptive act or practice under AS 45.50.471 - 45.50.561. Each day of a violation constitutes a separate violation.

(b) In an action brought under AS 45.50.531(a), a consumer whose personal data is subjected to unauthorized access, destruction, use, modification, or disclosure has suffered an ascertainable loss of money or property.

(c) The remedies provided under this section are in addition to the remedies provided under AS 45.48.080 for a violation of AS 45.48.010 - 45.48.090.

Sec. 45.48.870. Regulations. The attorney general may adopt regulations under AS 44.62 (Administrative Procedure Act) to implement AS 45.48.800 - 45.48.898.

Sec. 45.48.875. Exemptions. (a) AS 45.48.800 - 45.48.898 do not apply to

(1) protected health information that a covered entity or business associate collects or processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with, the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191) and regulations adopted under that Act; in this paragraph, "business associate," "covered entity," and "protected health information" have the meanings given in 45 C.F.R. 160.103;

(2) data collected, processed, or maintained that must be retained to administer benefits for another individual relating to an individual who is the subject of protected health information under (1) of this subsection and used for the purpose of administering the benefits;

(3) patient-identifying information under 42 U.S.C. 290dd-2;

(4) information that identifies a consumer that is collected, processed, or maintained in connection with

(A) activities that are subject to 45 C.F.R. Part 46 (Protection of Human Subjects);

(B) research on human subjects conducted under good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(C) activities that are subject to the protections provided in 21 C.F.R. Parts 50 and 56; or

(D) personal data used or shared in research, as that term is defined in 45 C.F.R. 164.501, that is conducted in accordance with the standards applicable under (A) - (C) of this paragraph or other research conducted in accordance with applicable law;

(5) information and documents created for purposes of 42 U.S.C. 11101 - 11152 (Health Care Quality Improvement Act of 1986) and related regulations;

(6) patient safety work product, as defined in 42 C.F.R. 3.20, that is created for purposes of improving patient safety under 42 C.F.R. Part 3 (Patient Safety Organizations and Patient Safety Work Product) and 42 U.S.C. 299b-21 - 299b-26 (Patient Safety and Quality Improvement Act of 2005);

(7) information derived from health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191) and related regulations;

(8) information collected, processed, or sold that is subject to 15 U.S.C. 6801 - 6827 (Gramm-Leach-Bliley Act) and related regulations;

(9) an activity that involves the collection, maintenance, disclosure, sale, communication, or use of any information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living and that is subject to 15 U.S.C. 1681 - 1681x (Fair Credit Reporting Act), if the activity is performed by

(A) a consumer reporting agency, as that term is defined in 15 U.S.C. 1681a(f);

(B) a person who furnishes information to a consumer reporting agency under 15 U.S.C. 1681s-2; or

(C) a person who uses a consumer report as provided in 15 U.S.C. 1681b(a)(3);

(10) personal data collected, processed, sold, or disclosed under 18 U.S.C. 2721 - 2725 (Driver's Privacy Protection Act of 1994) and related regulations;

(11) personal data regulated by 20 U.S.C. 1232g (Family Educational Rights and Privacy Act of 1974);

(12) personal data collected, processed, sold, or disclosed in compliance with 12 U.S.C. 2001 - 2279cc (Farm Credit System);

(13) data collected, processed, or maintained

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

(B) as the emergency contact information of an individual used for emergency contact purposes;

(14) personal data collected, processed, sold, or disclosed related to a price, route, or service of an air carrier, but only to the extent preempted by 49 U.S.C. 41713.

(b) AS 45.48.800 - 45.48.898 may not be construed to restrict the ability of a controller or processor to collect, process, transfer, or disclose a consumer's personal data to the extent necessary to

(1) comply with federal, state, municipal, or tribal law;

(2) comply with a civil, criminal, or regulatory inquiry or an investigation, subpoena, or summons by federal, state, municipal, or tribal authorities;

(3) cooperate with a law enforcement agency concerning conduct or activity that the person reasonably and in good faith believes may violate federal, state, municipal, or tribal law;

(4) investigate, establish, exercise, or defend a legal claim;

(5) provide a product or service specifically requested by the

consumer;

(6) perform under a contract to which the consumer is a party, including fulfilling the terms of a written warranty;

(7) take steps at the request of a consumer before entering into a contract;

(8) take immediate steps to protect an interest that is essential for the life or physical safety of an individual when the collection, processing, transfer, or disclosure cannot be manifestly justified using another legal basis;

(9) prevent, detect, protect against, or respond to a security incident or malicious, deceptive, fraudulent, or illegal activity or preserve the integrity or security of systems;

(10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all relevant laws and regulations governing that research and is approved, monitored, and governed by an institutional review board or similar independent oversight entity that determines whether

(A) the deletion of personal data requested by a consumer under AS 45.48.805(a)(4) is likely to provide substantial benefits that do not exclusively accrue to the controller;

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

(C) the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including risks associated with reidentification;

(11) assist another controller, processor, or third party with any obligations under AS 45.48.800 - 45.48.898;

(12) process personal data for reasons of public interest in the areas of public health, community health, or population health, but only to the extent that the processing is

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

(B) under the responsibility of a professional subject to

confidentiality obligations under federal, state, municipal, or tribal law;

(13) ensure the data security and integrity of personal data as required by AS 45.48.800 - 45.48.898, protect against spam, or protect and maintain networks and systems, including through diagnostics, debugging, and repairs;

(14) carry out a product recall under federal or state law or to fulfill a warranty;

(15) conduct medical research in compliance with 45 C.F.R. Part 46 (Protection of Human Subjects) or 21 C.F.R. Parts 50 and 56; or

(16) process personal data previously collected in accordance with AS 45.48.800 - 45.48.898 to convert the personal data into de-identified data, including to

(A) conduct internal research to develop, improve, or repair products, services, or technology;

(B) identify and repair technical errors that impair existing or intended functionality; or

(C) perform solely internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) A requirement under AS 45.48.800 - 45.48.898 does not apply if

(1) compliance would violate an evidentiary privilege under state law;

(2) a controller or processor provides personal data as part of a privileged communication to a person covered by an evidentiary privilege;

(3) the right or obligation would adversely affect a right of another person;

(4) a person collects or processes personal data in the course of that person's purely personal or household activities;

(5) compliance would require a private school as defined in AS 14.45.200 or a private institution of higher education as defined in 20 U.S.C. 1001

to delete personal data when that deletion would unreasonably interfere with the school's provision of educational services or ordinary operations;

(6) compliance would require the affirmative collection of personal data about the age of users that a controller does not already collect in the normal course of business or require a controller to implement age restriction requirements or age verification.

(d) A controller may collect or process personal data under this section only to the extent that the collection or processing

(1) is reasonably necessary for and proportionate to the purposes listed in this section or, in the case of sensitive data, strictly necessary for the purposes listed in this section;

(2) is limited to data that is necessary in relation to the specific purposes listed in this section;

(3) is subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers related to the processing of personal data; and

(4) complies with AS 45.48.805(d).

(e) A controller that collects or processes personal data under an exemption in this section bears the burden of demonstrating that the collection or processing qualifies for the exemption and complies with the requirements of (d) of this section.

(f) A violation of AS 45.48.800 - 45.48.898 by a processor or third-party controller that receives and processes personal data from a controller or another processor is not imputed to the controller or processor that disclosed the personal data unless the disclosing controller or processor had actual knowledge that the receiving processor or third-party controller would commit the violation. A violation of AS 45.48.800 - 45.48.898 by a controller or processor that discloses personal data to a third-party controller or processor is not imputed to the receiving third-party controller or processor.

Sec. 45.48.880. Component parts. If a series of steps or transactions are component parts of a single transaction and are intended from the beginning to avoid

the reach of AS 45.48.800 - 45.48.898, including a controller's disclosure of information to a third party to avoid being considered a sale of personal data, the steps or transactions may not be considered separate for the purposes of determining compliance with, an exception to, or a violation of AS 45.48.800 - 45.48.898.

Sec. 45.48.885. Provisions not waivable. A consumer's waiver of the provisions of AS 45.48.800 - 45.48.898 is contrary to public policy and is unenforceable and void. This section does not prevent a consumer from

(1) declining to request information from a controller;

(2) declining to request that a controller not collect, sell, or disclose the consumer's personal data; or

(3) authorizing a controller to sell the consumer's personal data after previously requesting that the controller not sell the personal data.

Sec. 45.48.890. Liberal construction. The intent of AS 45.48.800 - 45.48.898 is remedial, and its provisions shall be liberally construed.

Sec. 45.48.895. Definitions. In AS 45.48.800 - 45.48.898, unless the context clearly indicates otherwise,

(1) "affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by, or is under common control with another legal entity; in this paragraph, "control" and "controlled" mean having

(A) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a legal entity;

(B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(C) the power to exercise controlling influence over the management of a legal entity;

(2) "affirmative consent"

(A) means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous authorization for an act or practice, after having been informed, in response to a specific request from a controller; in making the request, the controller shall

(i) provide to the consumer a clear and conspicuous

stand-alone disclosure;

(ii) provide to the consumer a written request that describes the processing purpose for which the consumer's consent is sought, that clearly distinguishes between an act or practice that is necessary to fulfill a request of the consumer and an act or practice that is for another purpose, that clearly states the specific categories of personal data that the controller intends to collect, process, or transfer under each act or practice, and that uses easy-to-understand language with prominent headings that enable a reasonable consumer to identify and understand each act or practice;

(iii) clearly explain the consumer's rights related to consent;

(iv) make the request reasonably accessible to and usable by consumers with disabilities;

(v) make the request available to the consumer in each language in which the controller provides a product or service for which authorization is sought; and

(vi) ensure that the option to refuse to give consent is at least as prominent and takes the same or fewer steps as the option to give consent;

(B) does not include

(i) consent for an act or practice inferred from the inaction of the consumer or the consumer's continued use of a service or product provided by the controller;

(ii) acceptance of general or broad terms of use or a similar document that contains descriptions of personal data processing along with other unrelated information;

(iii) hovering over, muting, pausing, or closing a given piece of content on the Internet;

(iv) an agreement obtained through the use of a false, fraudulent, or materially misleading statement or representation; or

(v) an agreement obtained through the use of a dark pattern;

(3) "authenticate" means the use of reasonable means to determine that a request to exercise a right granted to a consumer under AS 45.48.800 - 45.48.898 is being made by, or on behalf of, the consumer who is entitled to exercise that right with respect to the personal data;

(4) "biometric data"

(A) means data generated by automatic measurements of an individual's fingerprint, voiceprint, retina, iris, gait, or other unique biological pattern or characteristic that can be used to identify a specific individual;

(B) does not include

(i) a digital or physical photograph;

(ii) an audio or video recording; or

(iii) data generated from a digital or physical photograph or an audio or video recording, unless the data is generated to identify a specific individual;

(5) "collect" means to buy, rent, gather, obtain, receive, access, or otherwise acquire personal data by any means;

(6) "commissioner" means the commissioner of commerce, community, and economic development;

(7) "consumer"

(A) means an individual who is a resident of the state;

(B) does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit organization, or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit organization, or government agency;

(8) "consumer health data" means personal data that describes or reveals a consumer's past, present, or future physical or mental health condition or diagnosis;

(9) "contextual advertising"

(A) means displaying or presenting an advertisement that does not vary based on the identity of the individual recipient and is based solely on

(i) the immediate content of an Internet website or online service within which the advertisement appears; or

(ii) a specific request of the consumer for information or feedback if displayed in proximity to the results of the request for information;

(B) does not include a controller's use of the following types of personal data to display a contextual advertisement without making inferences about the consumer, profiling the consumer, or using the data for any other purpose, if the consumer may use technical means to hide or change the consumer's physical location and to specify a language preference:

(i) technical specifications that are necessary for the advertisement to be delivered and display properly on a given device;

(ii) a consumer's immediate presence in a geographic area with a radius not smaller than 10 miles, or an area reasonably estimated to include online activity from at least 5,000 users, but not including precise geolocation data; or

(iii) the consumer's language preferences, as inferred from context, browser settings, or user settings;

(10) "controller" means a person who, alone or jointly with others, determines the purpose and means of collecting or processing personal data;

(11) "dark pattern" means

(A) a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice; and

(B) a practice the Federal Trade Commission refers to as a "dark pattern";

(12) "data broker" means a controller that knowingly collects and sells to third parties the personal data of a consumer with whom the controller does not

have a direct relationship, but does not include a consumer reporting agency to the extent the agency is covered by 15 U.S.C. 1681 et seq. (Fair Credit Reporting Act);

(13) "de-identified data" means data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual or a device linked to the individual and for which the controller holding the information

(A) takes reasonable physical, administrative, and technical measures to ensure that the data cannot be associated with an individual or be used to reidentify an individual or device that identifies or is linked, or is reasonably linkable, to an individual;

(B) publicly commits to process the data only in a de-identified fashion and does not attempt to reidentify the data; and

(C) contractually obligates a recipient of the data to satisfy the criteria set out in (A) and (B) of this paragraph;

(14) "department" means the Department of Commerce, Community, and Economic Development;

(15) "first party" means a consumer-facing controller with which the consumer intends or expects to interact;

(16) "first-party advertising" means

(A) processing of first-party data by the first party for the purposes of advertising and marketing

(i) through mail, electronic mail, text message, or other direct communication with a consumer;

(ii) in a physical location operated by the first party; or

(iii) through display or presentation of an advertisement on the first party's own Internet website, application, or other online content; and

(B) a marketing measurement related to advertising and marketing under (A) of this paragraph;

(17) "first-party data" means personal data collected directly from a consumer by a first party;

(18) "identified or identifiable individual" means an individual who can be readily identified, directly or indirectly;

(19) "marketing measurement" means measuring and reporting on marketing performance or media performance by the controller and processing of personal data by the controller for measurement and reporting of frequency, attribution, and performance;

(20) "minor" means a consumer who is under 18 years of age;

(21) "personal data"

(A) means information that is linked, or is reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or a device that identifies or is linked, or is reasonably linkable, to an individual;

(B) does not include publicly available information or de-identified data;

(22) "precise geolocation data"

(A) means information derived from a global positioning system or other technology capable of determining with specificity the latitude and longitude coordinates or other spatial location of an individual or device and that reveals, with precision and accuracy within a radius of 1,750 feet or less, the past or present physical location of

(i) an individual; or

(ii) a device that identifies one or more individuals or is linked, or reasonably linkable, to one or more individuals;

(B) does not include

(i) the content of communications, a photograph or video, or metadata associated with a photograph or video that cannot be linked to an individual; or

(ii) information generated by or connected to an advanced utility metering infrastructure system or equipment for use by a utility;

(23) "process" and "processing" mean any operation or set of

operations performed on personal data or on sets of personal data, whether or not by automated means;

(24) "processor" means a person who collects, processes, or transfers personal data on behalf of, and at the direction of, a controller, another processor, or a federal, state, municipal, or tribal government;

(25) "profiling" means a form of processing performed on personal data to evaluate, analyze, or predict an individual's economic situation, health, personal preferences, interests, reliability, behavior, location, movements, or other personal features;

(26) "publicly available information"

(A) means information that is lawfully made available to the general public from

(i) federal, state, municipal, or tribal government records, if the information is collected, processed, and transferred in accordance with any restrictions or terms of use placed on the information by the relevant government;

(ii) widely distributed media; or

(iii) a disclosure to the general public as required by federal, state, municipal, or tribal law;

(B) does not include

(i) material that constitutes an obscene visual depiction under 18 U.S.C. 1460;

(ii) an inference made exclusively from multiple independent sources of publicly available information that reveals sensitive data pertaining to a consumer;

(iii) biometric data;

(iv) personal data created through the combination of information under (A) of this paragraph with personal data that is not publicly available information;

(v) genetic data, unless otherwise made available to the public by the individual to whom the information pertains;

(vi) information made available by a consumer on an Internet website or online service that is available to all members of the public, with or without charge, when the consumer has restricted the information to a specific audience; or

(vii) authentic or computer-generated intimate images known to be nonconsensual;

(27) "sale of personal data"

(A) means an exchange of personal data for monetary or other valuable consideration by a controller to a third party;

(B) does not include

(i) the disclosure of personal data to a processor that processes the personal data on behalf of a controller;

(ii) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

(iii) the disclosure or transfer of personal data to an affiliate of a controller;

(iv) the disclosure of personal data, with the consumer's affirmative consent, when the consumer affirmatively directs a controller to disclose the personal data or intentionally uses a controller to interact with a third party; or

(v) the disclosure of personal data that the consumer intentionally made available to the general public through mass media and did not restrict to a specific audience;

(28) "sensitive data" means personal data that

(A) reveals a consumer's racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, status as pregnant, sexual orientation, status as transgender or nonbinary, union membership, or citizenship or immigration status;

(B) contains consumer health data;

(C) contains a consumer's genetic or biometric data;

(D) pertains to a consumer that a controller knows or should

know, based on knowledge fairly implied under objective circumstances, is a minor;

(E) contains precise geolocation data;

(F) contains a consumer's social security number, driver's license number, known traveler number, state identification card number, passport number, or other government-issued identifier that is not required by law to be displayed in public;

(G) reveals the online activities of a consumer or device linked, or reasonably linkable, to a consumer, over time and across Internet websites, online applications, or mobile applications that do not share common branding, or data generated by profiling those online activities;

(29) "targeted advertising"

(A) means

(i) displaying or presenting an online advertisement to a consumer, to a device identified by a unique persistent identifier, or to a group of consumers or devices identified by unique persistent identifiers if the advertisement is selected based, in whole or in part, on known or predicted preferences, characteristics, behavior, or interests associated with the consumer or consumers or the device;

(ii) displaying or presenting an online advertisement for a product or service based on the previous interaction of a consumer or a device identified by a unique persistent identifier with the product or service on an Internet website or online service that does not share common branding with the Internet website or online service displaying or presenting the advertisement; or

(iii) a marketing measurement related to advertising under (i) and (ii) of this subparagraph;

(B) does not include first-party advertising or contextual advertising;

(30) "third party"

(A) means a person who collects personal data from another

person who is not the consumer to whom the data pertains;

(B) does not include

(i) a processor with respect to the personal data; or

(ii) a person who collects personal data from another entity if the two entities are affiliates;

(31) "transfer" means to disclose, release, disseminate, make available, license, rent, or share personal data to a third party by any means;

(32) "unique persistent identifier"

(A) includes a device identifier; an Internet protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers; or other forms of persistent or probabilistic identifiers that are reasonably linkable to one or more consumers or devices that identify or are reasonably linkable to one or more consumers;

(B) does not include an identifier assigned by a controller for the sole purpose of giving effect to the exercise of affirmative consent or opt out by a consumer

(i) pertaining to the collection, processing, and transfer of personal data; or

(ii) otherwise limiting the collection, processing, or transfer of personal data.

Sec. 45.48.898. Short title. AS 45.48.800 - 45.48.898 may be cited as the Alaska Data Privacy Act.

*** Sec. 6.** AS 45.50.471(b) is amended by adding a new paragraph to read:

(58) violating AS 45.48.800 - 45.48.898 (Alaska Data Privacy Act).

*** Sec. 7.** The uncodified law of the State of Alaska is amended by adding a new section to read:

APPLICABILITY: CONTRACTS. This Act applies to a contract entered into on or after the effective date of this Act.

*** Sec. 8.** The uncodified law of the State of Alaska is amended by adding a new section to read:

TRANSITION: DATA PROTECTION ASSESSMENTS. A data protection assessment required under AS 45.48.835, added by sec. 5 of this Act, is not required for a processing activity until January 1, 2028.

*** Sec. 9.** This Act takes effect January 1, 2027.