AN ACT ESTABLISHING THE CONSUMER DATA PRIVACY ACT; PROVIDING DEFINITIONS; ESTABLISHING APPLICABILITY; PROVIDING FOR CONSUMER RIGHTS TO PERSONAL DATA; ESTABLISHING REQUIREMENTS AND LIMITATIONS FOR A CONTROLLER OF PERSONAL DATA; ESTABLISHING REQUIREMENTS AND LIMITATIONS FOR A PROCESSOR OF PERSONAL DATA; PROVIDING FOR DATA PROTECTION ASSESSMENTS; PROVIDING EXEMPTIONS AND COMPLIANCE REQUIREMENTS; PROVIDING FOR ENFORCEMENT; AND PROVIDING A DELAYED EFFECTIVE DATE AND A TERMINATION DATE.

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

Section 1. Short title. [Sections 1 through 12] may be cited as the "Consumer Data Privacy Act".

Section 2. Definitions. As used in [sections 1 through 12], unless the context clearly indicates otherwise, the following definitions apply:

(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.

(2) "Authenticate" means to use reasonable methods to determine that a request to exercise any of the rights afforded under [section 5(1)(a) through (1)(e)] is being made by, or on behalf of, the consumer who is entitled to exercise these consumer rights with respect to the personal data at issue.

(3) (a) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual.

(b) The term does not include:

(i) a digital or physical photograph;

(ii) an audio or video recording; or

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

(4) "Child" means an individual under 13 years of age.

(5) (a) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer. The term may include a written statement, a statement by electronic means, or any other unambiguous affirmative action.

(b) The term does not include:

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

(ii) hovering over, muting, pausing, or closing a given piece of content; or

(iii) an agreement obtained using dark patterns.

(6) (a) "Consumer" means an individual who is a resident of this state.

(b) The term 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, 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, or government agency.

(7) "Control" or "controlled" means:

(a) ownership of or the power to vote more than 50% of the outstanding shares of any class of voting security of a company;

(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 company.

(8) "Controller" means an individual who or legal entity that, alone or jointly with others, determines the purpose and means of processing personal data.

(9) "Dark pattern" means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice.

(10) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to necessities such as food and water.

(11) "Deidentified data" means data that cannot be used to reasonably infer information about or otherwise be linked to an identified or identifiable individual or a device linked to the individual if the controller that possesses the data:

(a) takes reasonable measures to ensure that the data cannot be associated with an individual;

(b) publicly commits to process the data in a deidentified fashion only and to not attempt to reidentify the data; and

(c) contractually obligates any recipients of the data to satisfy the criteria set forth in subsections (11)(a) and (11)(b).

(12) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

(13) "Institution of higher education" means any individual who or school, board, association, limited liability company, or corporation that is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

(14) "Nonprofit organization" means any organization that is exempt from taxation under section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986 or any subsequent corresponding internal revenue code of the United States as amended from time to time.

(15) (a) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual.

(b) The term does not include deidentified data or publicly available information.

(16) (a) "Precise geolocation data" means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet.

(b) The term does not include the content of communications, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(17) "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(18) "Processor" means an individual who or legal entity that processes personal data on behalf of a controller.

(19) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(20) "Protected health information" has the same meaning as provided in the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996.

(21) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(22) "Publicly available information" means information that:

(a) is lawfully made available through federal, state, or municipal government records or widely distributed media; or

(b) a controller has a reasonable basis to believe a consumer has lawfully made available to the public.

(23) (a) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party.

(b) The term does not include:

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

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

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

(iv) the disclosure of personal data in which the consumer directs the controller to disclose the

personal data or intentionally uses the controller to interact with a third party;

(v) the disclosure of personal data that the consumer:

(A) intentionally made available to the public via a channel of mass media; and

(B) did not restrict to a specific audience; or

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

(24) "Sensitive data" means personal data that includes:

(a) data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, information about a person's sex life, sexual orientation, or citizenship or immigration status;

(b) the processing of genetic or biometric data for the purpose of uniquely identifying an individual;

(c) personal data collected from a known child; or

(d) precise geolocation data.

(25) (a) "Targeted advertising" means displaying advertisements to a consumer in which the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated internet websites or online applications to predict the consumer's preferences or interests.

(b) The term does not include:

(i) advertisements based on activities within a controller's own internet websites or online applications;

(ii) advertisements based on the context of a consumer's current search query or visit to an internet website or online application;

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

(iv) processing personal data solely to measure or report advertising frequency, performance, or reach.

(26) "Third party" means an individual or legal entity, such as a public authority, agency, or body, other than the consumer, controller, or processor or an affiliate of the controller or processor.

(27) "Trade secret" has the same meaning as provided in 30-14-402.

Section 3. Applicability. The provisions of [sections 1 through 12] apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and:

(1) control or process the personal data of not less than 50,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

(2) control or process the personal data of not less than 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data.

Section 4. Exemptions. (1) [Sections 1 through 12] do not apply to any:

(a) body, authority, board, bureau, commission, district, or agency of this state or any political subdivision of this state;

(b) nonprofit organization;

(c) institution of higher education;

(d) national securities association that is registered under 15 U.S.C. 78o-3 of the federal Securities Exchange Act of 1934, as amended;

(e) financial institution or an affiliate of a financial institution governed by, or personal data collected, processed, sold, or disclosed in accordance with, Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801, et seq.; or

(f) covered entity or business associate as defined in the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996, 45 CFR 160.103.

(2) Information and data exempt from [sections 1 through 12] include:

(a) protected health information under the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996;

(b) patient-identifying information for the purposes of 42 U.S.C. 290dd-2;

(c) identifiable private information for the purposes of the federal policy for the protection of human subjects of 1991, 45 CFR, part 46;

(d) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the international council for harmonisation of technical requirements for pharmaceuticals for human use;

(e) the protection of human subjects under 21 CFR, parts 6, 50, and 56, or personal data used or shared in research as defined in the federal Health Insurance Portability and Accountability Act of 1996, 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subsection (2)(e), or other research conducted in accordance with applicable law;

(f) information and documents created for the purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101, et seq.;

(g) patient safety work products for the purposes of the Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. 299b-21, et seq., as amended;

(h) information derived from any of the health care-related information listed in this subsection (2) that is:

(i) deidentified in accordance with the requirements for deidentification pursuant to the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996; or

(ii) included in a limited data set as described in 45 CFR 164.514(e), to the extent that the information is used, disclosed, and maintained in a manner specified in 45 CFR 164.514(e).

(i) information originating from and intermingled to be indistinguishable with or information treated in the same manner as information exempt under this subsection (2) that is maintained by a covered entity or business associate as defined in the privacy regulations of the federal Health Insurance Portability and Accountability Act of 1996, 45 CFR 160.103, or a program or qualified service organization, as specified in 42 U.S.C. 290dd-2, as amended;

(j) information used for public health activities and purposes as authorized by the federal Health Insurance Portability and Accountability Act of 1996, community health activities, and population health activities;

(k) the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that

provides information for use in a consumer report and by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. 1681, as amended;

(l) personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721, et seq., as amended;

(m) personal data regulated by the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g, et seq., as amended;

(n) personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act of 1993, 12 U.S.C. 2001, et seq., as amended;

(o) data processed or maintained:

(i) by an individual applying to, 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;

(ii) as the emergency contact information of an individual under [sections 1 through 12] and used for emergency contact purposes; or

(iii) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subsection (2)(a) and is used for the purposes of administering the benefits; and

(p) personal data collected, processed, sold, or disclosed in relation to price, route, or service, as these terms are used in the Airline Deregulation Act of 1978, 49 U.S.C. 40101, et seq., as amended, by an air carrier subject to the Airline Deregulation Act of 1978, to the extent [sections 1 through 12] are preempted by the Airline Deregulation Act of 1978, 49 U.S.C. 41713, as amended.

(3) Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et seq., shall be considered compliant with any obligation to obtain parental consent pursuant to [sections 1 through 12].

Section 5. Consumer personal data -- opt-out -- compliance -- appeals. (1) A consumer must have the right to:

(a) confirm whether a controller is processing the consumer's personal data and access the consumer's personal data, unless such confirmation or access would require the controller to reveal a trade secret;

(b) correct inaccuracies in the consumer's personal data, considering the nature of the personal data and the purposes of the processing of the consumer's personal data;

(c) delete personal data about the consumer;

(d) obtain a copy of the consumer's personal data previously provided by the consumer to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal data to another controller without hindrance when the processing is carried out by automated means, provided the controller is not required to reveal any trade secret; and

(e) opt out of the processing of the consumer's personal data for the purposes of:

(i) targeted advertising;

(ii) the sale of the consumer's personal data, except as provided in [section 7(2)]; or

(iii) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(2) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice.

(3) (a) A consumer may designate an authorized agent in accordance with [section 6] to exercise the rights of the consumer to opt out of the processing of the consumer's personal data under subsection (1)(e) on behalf of the consumer.

(b) A parent or legal guardian of a known child may exercise the consumer rights on the known child's behalf regarding the processing of personal data.

(c) A guardian or conservator of a consumer subject to a guardianship, conservatorship, or other protective arrangement, may exercise the rights on the consumer's behalf regarding the processing of personal data.

(4) Except as otherwise provided in [sections 1 through 12], a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to this section as follows:

(a) A controller shall respond to the consumer without undue delay, but not later than 45 days after

receipt of 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, provided the controller informs the consumer of the extension within the initial 45-day response period and the reason for the extension.

(b) If a controller declines to act regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to act and provide instructions for how to appeal the decision.

(c) Information provided in response to a consumer request must be provided by a controller, free of charge, once for each consumer during any 12-month period. If requests from a consumer are manifestly unfounded, excessive, technically infeasible, 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 the manifestly unfounded, excessive, technically infeasible, or repetitive nature of the request.

(d) If a controller is unable to authenticate a request to exercise any of the rights afforded under subsections (1)(a) through (1)(d) of this section using commercially reasonable efforts, the controller may not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right or rights until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the consumer's rights. A controller may not be required to authenticate an opt-out request, 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 notice to the person who made the request disclosing that the controller believes the request is fraudulent and that the controller may not comply with the request.

(e) A controller that has obtained personal data about a consumer from a source other than the consumer must be deemed in compliance with the consumer's request to delete the consumer's data pursuant to subsection (1)(c) by:

(i) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using the retained

data for any other purpose pursuant to the provisions of [sections 1 through 12]; or

(ii) opting the consumer out of the processing of the consumer's personal data for any purpose except for those exempted pursuant to the provisions of [sections 1 through 12].

(5) A controller shall establish a process for a consumer to appeal the controller's refusal to act on a request within a reasonable period after the consumer's receipt of the decision. The appeal process must be conspicuously available and like the process for submitting requests to initiate action pursuant to this section. Not later than 60 days after receipt of 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 also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

Section 6. Authorized agent. (1) A consumer may designate another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of the consumer's personal data for one or more of the purposes specified in [section 5(1)(e)]. The consumer may designate an authorized agent by way of a technology, including but not limited to an internet link or a browser setting, browser extension, or global device setting indicating a customer's intent to opt out of such processing.

(2) A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

(3) Opt-out methods must:

(a) provide a clear and conspicuous link on the controller's internet website to an internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and

(b) by no later than January 1, 2025, allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data through an opt-out preference signal sent with the consumer's consent, to the controller by a platform, technology, or mechanism that:

(i) may not unfairly disadvantage another controller;

(ii) may not make use of a default setting, but require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of a customer's personal data pursuant to [sections 1 through 12];

(iii) must be consumer-friendly and easy to use by the average consumer;

(iv) must be consistent with any federal or state law or regulation; and

(v) must allow the controller to accurately determine whether the consumer is a resident of the state and whether the consumer has made a legitimate request to opt out of any sale of a consumer's personal data or targeted advertising.

(4) (a) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of personal data, through an opt-out preference signal sent in accordance with the provisions of subsection (3) conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts, or club card program, the controller shall comply with the consumer's opt-out preference signal but may notify the consumer of the conflict and provide the choice to confirm controller-specific privacy settings or participation in such a program.

(b) If a controller responds to consumer opt-out requests received in accordance with subsection (3) by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subsection (3) for the retention, use, sale, or sharing of the consumer's personal data.

Section 7. Data processing by controller -- limitations. (1) A controller shall:

(a) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the personal data is processed, as disclosed to the consumer;

(b) 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; and

(c) provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and,

on revocation of the consent, cease to process the personal data as soon as practicable, but not later than 45 days after the receipt of the request.

(2) A controller may not:

(a) except as otherwise provided in [sections 1 through 12], process personal data for purposes that are not reasonably necessary to or compatible with the disclosed purposes for which the personal data is processed as disclosed to the consumer unless the controller obtains the consumer's consent;

(b) process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of the processing of sensitive data concerning a known child, without processing the sensitive data in accordance with the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et seq.;

(c) process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers;

(d) process the personal data of a consumer for the purposes of targeted advertising or sell the consumer's personal data without the consumer's consent under circumstances in which a controller has actual knowledge that the consumer is at least 13 years of age but younger than 16 years of age; or

(e) discriminate against a consumer for exercising any of the consumer rights contained in [sections 1 through 12], including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

(3) Nothing in subsection (1) or (2) may be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised their right to opt out pursuant to [sections 1 through 12] or the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(4) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the processing, as well as the way a consumer may exercise the right to opt out of the processing.

(5) A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(a) the categories of personal data processed by the controller;

(b) the purpose for processing personal data;

(c) the categories of personal data that the controller shares with third parties, if any;

(d) the categories of third parties, if any, with which the controller shares personal data; and

(e) an active e-mail address or other mechanism that the consumer may use to contact the controller; and

(f) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision regarding the consumer's request.

(6) (a) A controller shall establish and describe in a privacy notice one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to [sections 1 through 12] considering the ways in which consumers normally interact with the controller, the need for secure and reliable communication of consumer requests, and the ability of the controller to verify the identity of the consumer making the request.

(b) A controller may not require a consumer to create a new account to exercise consumer rights but may require a consumer to use an existing account.

Section 8. Data processor -- allowances -- limitations. (1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under [sections 1 through 12] to include:

(a) considering the nature of processing and the information available to the processor by appropriate technical and organizational measures as much as reasonably practicable to fulfill the controller's obligation to respond to consumer rights requests;

(b) considering the nature of processing and the information available to the processor by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as provided for in 30-14-1704, of the system of the processor to meet the controller's obligations; and

(c) providing necessary information to enable the controller to conduct and document data protection assessments.

(2) A contract between a controller and a processor must govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must be binding and clearly set forth 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 contract must also require that the processor:

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

(b) 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;

(c) on the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations in [sections 1 through 12];

(d) engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and

(e) allow and cooperate with reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to assess the processor's policies and technical and organizational measures in support of the obligations under [sections 1 through 12] using an appropriate and accepted control standard or framework and assessment procedure for the assessments. The processor shall provide a report of the assessment to the controller on request.

(3) Nothing in this section may be construed to relieve 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 [sections 1 through 12].

(4) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends on the following context in which personal data is to be processed:

(a) A person who is not limited in the processing of personal data pursuant to a controller's instructions or who fails to adhere to a controller's instructions is a controller and not a processor with respect to a specific processing of data.

(b) A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

(c) If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing and may be subject to an enforcement action under [section 12].

Section 9. Data protection assessment. (1) 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. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:

(a) the processing of personal data for the purposes of targeted advertising;

(b) the sale of personal data;

(c) the processing of personal data for the purposes of profiling in which the profiling presents a reasonably foreseeable risk of:

(i) unfair or deceptive treatment of or unlawful disparate impact on consumers;

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

(iii) a physical or other form of intrusion on the solitude or seclusion or the private affairs or concerns of consumers in which the intrusion would be offensive to a reasonable person; or

(iv) other substantial injury to consumers; and

(d) the processing of sensitive data.

(2) (a) Data protection assessments conducted pursuant to subsection (1) must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing as mitigated by safeguards that may be employed by the controller to reduce these risks.

(b) The controller shall factor into any data protection assessment the use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(3) (a) The attorney general may require that a controller disclose any 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.

(b) The attorney general may evaluate the data protection assessment for compliance with the responsibilities set forth in [sections 1 through 12].

(c) Data protection assessments are confidential and are exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552.

(d) To the extent any information contained in a data protection assessment disclosed to the attorney general includes information subject to attorney-client privilege or work product protection, the disclosure may not constitute a waiver of the privilege or protection.

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

(5) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment must be considered to satisfy the requirements established in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(6) Data protection assessment requirements must apply to processing activities created or generated after January 1, 2025, and are not retroactive.

Section 10. Deidentified data. (1) Any controller in possession of deidentified data shall:

(a) take reasonable measures to ensure that the deidentified data cannot be associated with an individual;

(b) publicly commit to maintaining and using deidentified data without attempting to reidentify the deidentified data; and

(c) contractually obligate any recipients of the deidentified data to comply with all provisions of [sections 1 through 12].

(2) Nothing in [sections 1 through 12] may be construed to:

(a) require a controller or processor to reidentify deidentified data or pseudonymous data; or

(b) maintain data in identifiable form or collect, obtain, retain, or access any data or technology to

be capable of associating an authenticated consumer request with personal data.

(3) Nothing in [sections 1 through 12] may be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

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

(b) 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; and

(c) does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(4) The rights afforded under [section 5(1)(a) through (1)(d)] may not apply to pseudonymous data in cases in which the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

(5) A controller that discloses pseudonymous data or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

Section 11. Compliance by controller or processor. (1) Nothing in [sections 1 through 12] may be construed to restrict a controller's or processor's ability to:

(a) comply with federal, state, or municipal ordinances or regulations;

(b) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal, or other government authorities;

(c) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or municipal ordinances or regulations;

(d) investigate, establish, exercise, prepare for, or defend legal claims;

(e) provide a product or service specifically requested by a consumer;

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

(g) take steps at the request of a consumer prior to entering a contract;

(h) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual and when the processing cannot be manifestly based on another legal basis;

(i) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any of these actions;

(j) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines or similar independent oversight entities that determine:

(A) whether the deletion of the information 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) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification;

(k) assist another controller, processor, or third party with any of the obligations under [sections 1 through 12]; or

(l) process personal data for reasons of public interest in public health, community health, or population health, but solely 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, or local law.

(2) The obligations imposed on controllers or processors under [sections 1 through 12] may not restrict a controller's or processor's ability to collect, use, or retain personal data for internal use to:

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

(b) effectuate a product recall;

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

(d) perform 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.

(3) The obligations imposed on controllers or processors under [sections 1 through 12] may not apply when compliance by the controller or processor with [sections 1 through 12] would violate an evidentiary privilege under the laws of this state. Nothing in [sections 1 through 12] may be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

(4) A controller or processor that discloses personal data to a processor or third-party controller in accordance with [sections 1 through 12] may not be considered to have violated [sections 1 through 12] if the processor or third-party controller that receives and processes the personal data violates [sections 1 through 12] provided, at the time the disclosing controller or processor disclosed the personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller would violate [sections 1 through 12]. A receiving processor or third-party controller receiving personal data from a disclosing controller or processor in compliance with [sections 1 through 12] is likewise not in violation of [sections 1 through 12] for the transgressions of the disclosing controller or processor from which the receiving processor or third-party controller receives the personal data.

(5) Nothing in [sections 1 through 12] may be construed to:

(a) impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including but not limited to the rights of any person:

(i) to freedom of speech or freedom of the press guaranteed in the first amendment to the United States constitution; or

(ii) under Rule 504 of the Montana Rules of Evidence; or

(b) apply to a person's processing of personal data during the person's personal or household activities.

(6) Personal data processed by a controller pursuant to this section may be processed to the extent that the processing is:

(a) reasonably necessary and proportionate to the purposes listed in this section; and

(b) adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. The controller or processor must, when applicable, consider the nature and purpose of the collection, use, or retention of the personal data collected, used, or retained pursuant to subsection (2). The personal data must be 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 relating to the collection, use, or retention of personal data.

(7) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements in subsection (6).

(8) Processing personal data for the purposes expressly identified in this section may not solely make a legal entity a controller with respect to the processing.

Section 12. Enforcement. (1) The attorney general has exclusive authority to enforce violations pursuant to [sections 1 through 11].

(2) (a) The attorney general shall, prior to initiating any action for a violation of any provision of [sections 1 through 11], issue a notice of violation to the controller.

(b) If the controller fails to correct the violation within 60 days of receipt of the notice of violation, the attorney general may bring an action pursuant to this section.

(c) If within the 60-day period the controller corrects the noticed violation and provides the attorney general an express written statement that the alleged violations have been corrected and that no such further violations will occur, no action must be initiated against the controller.

(3) Nothing in [sections 1 through 11] may be construed as providing the basis for or be subject to a private right of action for violations of [sections 1 through 11] or any other law.

Section 13. Codification instruction. [Sections 1 through 12] are intended to be codified as an

integral part of Title 30, chapter 14, and the provisions of Title 30, chapter 14, apply to [sections 1 through 12].

Section 14. Effective date. [This act] is effective October 1, 2024.

Section 15. Termination. [Section 12(2)] terminates April 1, 2026.

- END -

I hereby certify that the within bill,

SB 384, originated in the Senate.

_____

Secretary of the Senate

_____

President of the Senate

Signed this _____day

of_____, 2023.

_____

Speaker of the House

Signed this _____day

of_____, 2023.

SENATE BILL NO. 384

INTRODUCED BY D. ZOLNIKOV, K. REGIER, E. BOLDMAN, S. MORIGEAU, K. BOGNER, K. SULLIVAN, K. ZOLNIKOV, D. EMRICH

AN ACT ESTABLISHING THE CONSUMER DATA PRIVACY ACT; PROVIDING DEFINITIONS; ESTABLISHING APPLICABILITY; PROVIDING FOR CONSUMER RIGHTS TO PERSONAL DATA; ESTABLISHING REQUIREMENTS AND LIMITATIONS FOR A CONTROLLER OF PERSONAL DATA; ESTABLISHING REQUIREMENTS AND LIMITATIONS FOR A PROCESSOR OF PERSONAL DATA; PROVIDING FOR DATA PROTECTION ASSESSMENTS; PROVIDING EXEMPTIONS AND COMPLIANCE REQUIREMENTS; PROVIDING FOR ENFORCEMENT; AND PROVIDING A DELAYED EFFECTIVE DATE AND A TERMINATION DATE.