AN ACT GENERALLY REVISING PRIVACY LAWS; PROVIDING DEFINITIONS; REQUIRING NOTIFICATION TO CONSUMERS THAT CERTAIN INFORMATION HAS BEEN COLLECTED; REQUIRING AN OPT-OUT OPTION FOR CONSUMERS; REQUIRING A PRIVACY NOTICE FROM CONTROLLERS; REQUIRING THE ATTORNEY GENERAL TO POST RIGHTS AND RESPONSIBILITIES INFORMATION ONLINE; SPECIFYING CONTROLLER DUTIES; SPECIFYING RESPONSIBILITIES BY ROLE; AMENDING SECTIONS 20-7-1324, 30-14-2802, 30-14-2803, 30-14-2804, 30-14-2808, 30-14-2812, 30-14-2816, AND 30-14-2817, MCA; AND REPEALING SECTION 15, CHAPTER 681, LAWS OF 2023."

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

Section 1. Section 20-7-1324, MCA, is amended to read:

"**20-7-1324. Definitions.** As used in 20-7-1323 through 20-7-1326, the following definitions apply:

(1) "Deidentified information" means information that cannot be used to identify an individual pupil.

(2) "K-12 online application" means an internet website, online service, cloud computing service, online application, or mobile application that is used primarily for K-12 school purposes and that was designed and is marketed for K-12 school purposes.

(3) (a) "K-12 school purposes" means activities that customarily take place at the direction of a school, teacher, or school district or aid in the administration of school activities, including but not limited to instruction in the classroom or at home, administrative activities, and collaboration between pupils, school personnel, or parents, or that are for the use and benefit of a school.

(b) The term does not include courses that are provided for the purpose of postsecondary credit or work-based learning courses provided by a work-based learning partner pursuant to 20-7-1510.

(4) "Operator" means the operator of a K-12 online application who knows or reasonably should know that the application is used primarily for K-12 school purposes.

(5) (a) "Protected information" means personally identifiable information or materials, in any media or format, that describes or otherwise identifies a pupil and that is:

(i) created or provided by a pupil, or the pupil's parent or legal guardian, to an operator in the course of the pupil's, parent's, or legal guardian's use of the operator's K-12 online application;

(ii) created or provided by an employee or agent of a school district to an operator in the course of the employee's or agent's use of the operator's K-12 online application; or

(iii) gathered by an operator through the operator's K-12 online application.

(b) The term includes but is not limited to:

(i) information in the pupil's educational record or e-mail messages;

(ii) first and last name, home address, telephone number, e-mail address, or other information that allows physical or online contact;

(iii) discipline records, test results, special education data, juvenile dependency records, grades, or evaluations;

(iv) criminal, medical, or health records;

(v) social security number;

(vi) biometric information;

(vii) disability;

(viii) socioeconomic information;

(ix) food purchases;

(x) political affiliation;

(xi) religious information; or

(xii) text messages, documents, pupil identifiers, search activity, photos, voice recordings, or geolocation information.

(6) (a) "Pupil records" means:

(i) any information directly related to a pupil that is maintained by a school district; or

(ii) any information acquired directly from a pupil through the use of instructional software or applications assigned to the pupil by a teacher or other school district employee.

(b) The term does not include deidentified information, including aggregated deidentified

information used:

(i) by a third party to improve educational products for adaptive learning purposes and for customizing pupil learning;

(ii) to demonstrate the effectiveness of a third party's products in the marketing of those products; or

(iii) for the development and improvement of educational sites, services, or applications.

(7) (a) "Pupil-generated content" means materials created by a pupil, including but not limited to essays, research reports, portfolios, creative writing, music or other audio files, photographs, and account information that enables ongoing ownership of pupil content.

(b) The term does not include pupil responses to a standardized assessment for which pupil possession and control would jeopardize the validity and reliability of that assessment.

(8) "Third party" refers to a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records."

Section 2. Section 30-14-2802, MCA, is amended to read:

"**30-14-2802. Definitions.** As used in this part, unless the context clearly indicates otherwise, the following definitions apply:

(1) "Adult" means an individual who is 18 years of age or older.

~~(1)~~(2) "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)~~(3) "Authenticate" means to use reasonable methods to determine that a request to exercise any of the rights afforded under 30-14-2808(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)~~(4) (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)~~(5) "Child" means an individual under 13 years of age.

~~(5)~~(6) (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)~~(7) (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)~~(8) "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)~~(9) "Controller" means an individual who or legal entity that, alone or jointly with others, determines the purpose and means of processing personal data.

~~(9)~~(10) "Dark pattern" means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice.

~~(10)~~(11)"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)~~(12)"De-identified 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 de-identified fashion only and to not attempt to re-identify the data; and

(c) contractually obligates any recipients of the data to satisfy the criteria set forth in subsections ~~(11)(a)~~ (12)(a) and ~~(11)(b)~~ (12)(b).

(13) "Heightened risk of harm to minors" means processing the personal data of a minor in a manner that presents a reasonably foreseeable risk that could cause:

(a) unfair or deceptive treatment of or an unlawful disparate impact on a minor;

(b) financial, physical, or reputational injury to a minor;

(c) unauthorized disclosure of the personal data of a minor as a result of a security breach as described in 30-14-1704; or

(d) physical or other intrusion on the solitude or seclusion or the private affairs or concerns of a minor if the intrusion would be considered offensive to a reasonable person.

~~(12)~~(14)"Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

~~(13)~~(15)"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.

(16) "Minor" means a consumer who is under 18 years of age.

~~(14)~~(17)"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.

(18) (a) "Online service, product, or feature" means a service, product, or feature that is provided online.

(b) The term does not include:

(i) a telecommunications service as defined in 47 U.S.C. 153(53), as amended;

(ii) broadband internet access service as defined in 47 CFR 54.400(l), as amended; or

(iii) the delivery or use of a physical product.

~~(15)~~(19)(a) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual.

(b) The term does not include de-identified data or publicly available information.

~~(16)~~(20)(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)~~(21)"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)~~(22)"Processor" means an individual who or legal entity that processes personal data on behalf of a controller.

~~(19)~~(23)"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)~~(24)"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)~~(25)"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)~~(26)"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)~~(27)(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)~~(28)"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)~~(29)(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)~~(30)"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)~~(31)"Trade secret" has the same meaning as provided in 30-14-402."

Section 3. Section 30-14-2803, MCA, is amended to read:

"**30-14-2803. Applicability.** (1) The provisions of this part, excluding [sections 9 through 11], 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)~~(a) control or process the personal data of not less than ~~50,000~~ 25,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

~~(2)~~(b) control or process the personal data of not less than ~~25,000~~ 15,000 consumers and derive more than 25% of gross revenue from the sale of personal data.

(2) [Sections 9 through 11] apply to persons that conduct business in this state or deliver commercial products or services that are intentionally targeted to residents of this state."

Section 4. Section 30-14-2804, MCA, is amended to read:

"**30-14-2804. Exemptions.** (1) This part does 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 that is established to detect and prevent fraudulent acts in connection with insurance;

(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) state or federally chartered bank or credit union or an affiliate or subsidiary that is principally engaged in financial activities as described in 12 U.S.C. 1843(k);

~~(e)~~(f) ~~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)~~(g) 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

(h) insurer, as defined in 33-1-201, an insurance producer, as defined in 33-17-102, a third-party administrator of self-insurance, or an affiliate or subsidiary of an entity identified in this subsection (1)(h) that is principally engaged in financial activities, as described in 12 U.S.C. 1843(k), except that this subsection (1)(h) does not apply to a person who, alone or in combination with another person, establishes and maintains a self-insurance program that does not otherwise engage in the business of entering into policies of insurance.

(2) Information and data exempt from this part 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) de-identified in accordance with the requirements for de-identification 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 this part 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 this part is 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 this part."

Section 5. Section 30-14-2808, MCA, is amended to read:

"**30-14-2808. 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 30-14-2812(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 30-14-2809 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 this part, 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 this part; 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 this part.

(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."

(6) In response to a consumer request under subsection (1)(a), a controller may not disclose the following information about a consumer but shall inform the consumer instead with sufficient particularity that the controller has collected this information:

(a) social security number;

(b) driver's license number or other government-issued identification number;

(c) financial account number;

(d) health insurance account number or medical identification number;

(e) account password, security questions, or answer; or

(f) biometric data.

Section 6. Section 30-14-2812, MCA, is amended to read:

"**30-14-2812. 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 this part, 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 or willfully disregards 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 this part, 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 this part 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~~ in its privacy notice and provide access to a clear

and conspicuous method outside the privacy notice for a consumer to opt out of the sale or processing. This method may include but is not limited to an internet hyperlink clearly labeled "your opt-out rights" or "your privacy rights" that directly effectuates the opt-out request or takes consumers to a web page where the consumer can make the opt-out request.

(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 sells to or shares with third parties, if any;

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

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

(f) an explanation of the rights provided by 30-14-2808(1) and how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision regarding the consumer's request~~.~~ ; and

(g) the date the privacy notice was last updated.

(6) The privacy notice must be made available to the public in each language in which the controller provides a product or service that is subject to the privacy notice or carries out activities related to the product or service.

(7) The controller shall provide the privacy notice in a manner that is reasonably accessible to and usable by individuals with disabilities.

(8) Whenever a controller makes a material change to the controller's privacy notice or practices, the controller shall notify consumers affected by the material change with respect to any prospectively collected personal data and provide a reasonable opportunity for consumers to withdraw consent to any further materially different collection, processing, or transfer of previously collected personal data under the changed policy. The controller shall take all reasonable electronic measures to provide notification regarding material changes to affected consumers, taking into account available technology and the nature of the relationship.

(9) A controller is not required to provide a separate Montana-specific privacy notice or section of a privacy notice if the controller's general privacy notice contains all the information required by this section.

(10) The privacy notice must be posted online through a conspicuous hyperlink using the word "privacy" on the controller's website homepage or on a mobile device's application store page or download page. A controller that maintains an application on a mobile device or other device shall also include a hyperlink to the privacy notice in the application's settings menu or in a similarly conspicuous and accessible location. A controller that does not operate a website shall make the privacy notice conspicuously available to consumers through a medium regularly used by the controller to interact with consumers, including but not limited to mail.

~~(6)~~(11) (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 this part 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 7. Section 30-14-2816, MCA, is amended to read:

"**30-14-2816. Compliance by controller or processor.** (1) Nothing in this part 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)~~(i) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

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

~~(C)~~(iii) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

(k) assist another controller, processor, or third party with any of the obligations under this part; 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)~~(i) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and

~~(B)~~(ii) 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 this part 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 this part may not apply when compliance by the controller or processor with this part would violate an evidentiary privilege under the laws of this state. Nothing in this part 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 this part may not be considered to have violated this part if the processor or third-party controller that receives and processes the personal data violates this part 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 this part. A receiving processor or third-party controller receiving personal data from a disclosing controller or processor in compliance with this part is likewise not in violation of this part 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 this part 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~~.~~ ; or

(c) require a controller or processor to implement an age verification or age-gating system or otherwise affirmatively collect the age of consumers, but a controller that chooses to conduct commercially reasonable age estimation to determine which consumers are minors is not liable for an erroneous age estimation.

(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 8. Section 30-14-2817, MCA, is amended to read:

"**30-14-2817. Enforcement.** (1) The attorney general has exclusive authority and may use the duties and powers provided by Title 30, chapter 14, parts 1 and 2, to enforce violations pursuant to this part.

(2) The attorney general shall post on the attorney general's website:

(a) information relating to:

(i) the responsibilities of a controller pursuant to this part;

(ii) the responsibilities of a processor pursuant to this part; and

(iii) a consumer's rights pursuant to this part; and

(b) an online mechanism through which a consumer may submit a complaint regarding consumer data privacy to the attorney general.

(3) (a) If the attorney general has reasonable cause to believe that a person has engaged in or is engaging in a violation of this part, the attorney general may issue a civil investigative demand pursuant to 30-14-113.

(b) As part of a civil investigative demand, the attorney general may request that a controller

disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. The attorney general may evaluate the data protection assessment for compliance with the requirements pursuant to this part.

~~(2) (a) The attorney general shall, prior to initiating any action for a violation of any provision of this part, 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.~~(4) Actions brought by the department to enforce this part are subject to the statute of limitations pursuant to 27-2-231.

~~(3)~~(5) Nothing in this part may be construed as providing the basis for or be subject to a private right of action for violations of this part or any other law. ~~(Subsection (2) terminates April 1, 2026--sec. 15, Ch. 681, L. 2023.)~~"

Section 9. Duties of controllers -- duty of care -- rebuttable presumption. (1) (a) A controller that offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor shall use reasonable care to avoid a heightened risk of harm to minors caused by the online service, product, or feature.

(b) In an enforcement action brought by the attorney general pursuant to 30-14-2817, there is a rebuttable presumption that a controller used reasonable care as required under this section if the controller complied with this section.

(2) Unless a controller has obtained consent in accordance with subsection (3), a controller that offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor may not:

(a) process a minor's personal data:

(i) for the purposes of:

(A) targeted advertising;

(B) the sale of personal data; or

(C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer;

(ii) for any processing purpose other than the processing purpose that the controller disclosed at the time the controller collected the minor's personal data or that is reasonably necessary for and compatible with the processing purpose that the controller disclosed at the time the controller collected the minor's personal data; or

(iii) for longer than is reasonably necessary to provide the online service, product, or feature;

(b) use a system design feature to significantly increase, sustain, or extend a minor's use of the online service, product, or feature; or

(c) collect a minor's precise geolocation data unless:

(i) the minor's precise geolocation data is reasonably necessary for the controller to provide the online service, product, or feature;

(ii) the controller only collects and retains the minor's precise geolocation data for the time necessary to provide the online service, product, or feature; and

(iii) the controller provides to the minor a signal indicating that the controller is collecting the minor's precise geolocation data and makes the signal available to the minor for the entire duration of the collection of the minor's precise geolocation data. This subsection (2)(c)(iii) does not apply to a service or application that is used by and under the direction of a ski area operator.

(3) (a) A controller may not engage in the activities described in subsection (2) unless the controller obtains:

(i) the minor's consent; or

(ii) if the minor is a child, the consent of the minor's parent or legal guardian. A controller that complies with the verifiable parental consent requirements established in the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501, et seq., as amended, and the regulations, rules, guidance, and exemptions adopted pursuant to this act, as amended, is considered to have satisfied any requirement to obtain parental consent under this subsection (3)(a)(ii).

(b) (i) A controller that offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor may not:

(A) provide a consent mechanism that is designed to substantially subvert or impair or is manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice; or

(B) except as provided in subsection (3)(b)(ii), offer a direct messaging apparatus for use by a minor without providing readily accessible and easy-to-use safeguards to limit the ability of an adult to send unsolicited communications to the minor with whom the adult is not connected.

(ii) Subsection (3)(b)(i)(B) does not apply to an online service, product, or feature of which the predominant or exclusive function is:

(A) electronic mail; or

(B) direct messaging consisting of text, photos, or videos that are sent between devices by electronic means in which messages are:

(I) shared between the sender and the recipient;

(II) only visible to the sender and the recipient; and

(III) not posted publicly.

(4) Subsections (2)(a) and (2)(b) do not apply to a service or application that is used by and under the direction of an educational entity, including a learning management system or a student engagement program.

Section 10. Responsibility according to role -- processing data of minors. (1) A processor shall adhere to the instructions of a controller and shall assist the controller to meet the controller's obligations under [sections 9 and 11], taking into account the nature of the processing and the information available to the processor. The processor shall assist the controller by:

(a) taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligations under [section 9]; and

(b) providing information to enable the controller to conduct and document data protection assessments pursuant to [section 11].

(2) A contract between a controller and a processor must satisfy the requirements of 30-14-2813(2).

(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 9 and 11].

(4) Determining whether a person is acting as a controller or processor with respect to a specific processing of personal data is a fact-based determination that depends on the context in which personal data is to be processed. A person that is not limited in the person's processing of personal data pursuant to a controller's instructions or that fails to adhere to the instructions is a controller and not a processor with respect to a specific processing of personal 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 is a controller with respect to the processing and may be subject to an enforcement action under 30-14-2817.

Section 11. Data protection assessments for heightened risk of harm to minors. (1) A controller that, on or after October 1, 2025, offers an online service, product, or feature to a consumer whom the controller actually knows or willfully disregards is a minor shall conduct a data protection assessment for the online service, product, or feature if there is a heightened risk of harm to minors. The controller shall conduct the data protection assessment:

(a) in a manner that is consistent with the requirements established in 30-14-2814; and

(b) to address:

(i) the purpose of the online service, product, or feature;

(ii) the categories of a minor's personal data that the online service, product, or feature processes;

(iii) the purposes for which the controller processes a minor's personal data with respect to the online service, product, or feature; and

(iv) a heightened risk of harm to minors that is a reasonably foreseeable result of offering the online service, product, or feature to minors.

(2) A controller that conducts a data protection assessment pursuant to subsection (1) shall:

(a) review the data protection assessment as necessary to account for a material change to the processing operations of the online service, product, or feature that is the subject of the data protection assessment; and

(b) maintain documentation concerning the data protection assessment for the longer of:

(i) 3 years after the date on which the processing operations cease; or

(ii) the date the controller ceases offering the online service, product, or feature.

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

(4) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment is 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.

(5) If a controller conducts a data protection assessment pursuant to subsection (1) or a data protection assessment review pursuant to subsection (2)(a) and determines that the online service, product, or feature that is the subject of the assessment poses a heightened risk of harm to minors, the controller shall establish and implement a plan to mitigate or eliminate the heightened risk.

(6) (a) A data protection assessment conducted pursuant to this section:

(i) is confidential, except as provided in subsection (6)(b); and

(ii) is not a public record and is exempt from public inspection and copying under the Freedom of Information Act, 5 U.S.C. 552.

(b) (i) A controller shall make a data protection assessment conducted pursuant to this section available to the attorney general on request. The attorney general may evaluate the data protection assessment for compliance with this section and with other laws.

(ii) The disclosure of a data protection assessment pursuant to a request from the attorney general does not constitute a waiver of any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information in the assessment.

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

Section 12. Civil penalty injunction. (1) A violation of this part is a violation of Title 30, chapter 14, parts 1 and 2.

(2) A person who violates the provisions of this part following the 30-day period described in 30-14-2817(3) ~~or who breaches a written statement provided to the attorney general under 30-14-2817(4)(c)~~ is liable for a civil penalty in an amount not to exceed $7,500 for each violation.

(3) The attorney general may bring an action in the name of this state to:

(a) recover a civil penalty under this section;

(b) restrain or enjoin the person from violating this part; or

(c) recover the civil penalty and seek injunctive relief.

(4) The attorney general may recover reasonable attorney fees and other reasonable expenses incurred in investigating and bring an action under this section.

(5) The attorney general shall deposit a civil penalty collected under this section in a special revenue account to the credit of the department pursuant to 30-14-143.

Section 13. Statute of limitations. Actions brought by the department to enforce this part are subject to the statute of limitations pursuant to 27-2-231.

Section 14. Statute of limitations. Actions brought by the department to enforce this part are subject to the statute of limitations pursuant to 27-2-231.

Section 15. Repealer. Section 15, Chapter 681, Laws of 2023, is repealed.

Section 16. Codification instruction. (1) [Sections 9 through 12] are intended to be codified as an integral part of Title 30, chapter 14, part 28, and the provisions of Title 30, chapter 14, part 28, apply to [sections 9 through 12].

(2) [Section 13] is intended to be codified as an integral part of Title 30, chapter 14, part 1, and the provisions of Title 30, chapter 14, part 1, apply to [section 13].

(3) [Section 14] is intended to be codified as an integral part of Title 30, chapter 14, part 2, and the provisions of Title 30, chapter 14, part 2, apply to [section 14].

- END -

I hereby certify that the within bill,

SB 297, originated in the Senate.

_____

Secretary of the Senate

_____

President of the Senate

Signed this _____day

of_____, 2025.

_____

Speaker of the House

Signed this _____day
of_____, 2025.

SENATE BILL NO. 297

INTRODUCED BY D. ZOLNIKOV

AN ACT GENERALLY REVISING PRIVACY LAWS; PROVIDING DEFINITIONS; REQUIRING NOTIFICATION TO CONSUMERS THAT CERTAIN INFORMATION HAS BEEN COLLECTED; REQUIRING AN OPT-OUT OPTION FOR CONSUMERS; REQUIRING A PRIVACY NOTICE FROM CONTROLLERS; REQUIRING THE ATTORNEY GENERAL TO POST RIGHTS AND RESPONSIBILITIES INFORMATION ONLINE; SPECIFYING CONTROLLER DUTIES; SPECIFYING RESPONSIBILITIES BY ROLE; AMENDING SECTIONS 20-7-1324, 30-14-2802, 30-14-2803, 30-14-2804, 30-14-2808, 30-14-2812, 30-14-2816, AND 30-14-2817, MCA; AND REPEALING SECTION 15, CHAPTER 681, LAWS OF 2023."