CHAPTER 369

AN ACT SB 619

Relating to protections for the personal data of consumers; creating new provisions; and amending ORS 180.095.

Be It Enacted by the People of the State of Oregon:

SECTION 1. As used in sections 1 to 9 of this 2023 Act:

(1) "Affiliate" means a person that, directly or indirectly through one or more intermediaries, controls, is controlled by or is under common control with another person such that:

(a) The person owns or has the power to vote more than 50 percent of the outstanding shares of any voting class of the other person's securities;

(b) The person has the power to elect or influence the election of a majority of the directors, members or managers of the other person;

(c) The person has the power to direct the management of another person; or

(d) The person is subject to another person's exercise of the powers described in paragraph (a), (b) or (c) of this subsection.

(2) "Authenticate" means to determine, using commercially reasonable methods, whether a consumer with the rights described in section 3 of this 2023 Act, or a person acting on behalf of the consumer, is the consumer who has asked to exercise, or is a person who has authority to exercise, any of the consumer's rights.

(3)(a) "Biometric data" means personal data generated by automatic measurements of a consumer's biological characteristics, such as the consumer's fingerprint, voiceprint, retinal pattern, iris pattern, gait or other unique biological characteristics that allow or confirm the unique identification of the consumer.

(b) "Biometric data" does not include:

(A) A photograph recorded digitally or otherwise;

(B) An audio or video recording;

(C) Data from a photograph or from an audio or video recording, unless the data were generated for the purpose of identifying a specific consumer or were used to identify a particular consumer; or

(D) Facial mapping or facial geometry, unless the facial mapping or facial geometry was generated for the purpose of identifying a specific consumer or was used to identify a specific consumer.

(4) "Business associate" has the meaning given that term in 45 C.F.R. 160.103, as in effect on the effective date of this 2023 Act.

(5) "Child" means an individual under the age of 13.

(6) "Consent" means an affirmative act by means of which a consumer clearly and conspicuously communicates the consumer's freely given, specific, informed and unambiguous assent to another person's act or practice under the following conditions:

(a) The user interface by means of which the consumer performs the act does not have any mechanism that has the purpose or substantial effect of obtaining consent by obscuring, subverting or impairing the consumer's autonomy, decision-making or choice; and

(b) The consumer's inaction does not constitute consent.

(7) "Consumer" means a natural person who resides in this state and acts in any capacity other than in a commercial or employment context.

(8) "Controller" means a person that, alone or jointly with another person, determines the purposes and means for processing personal data.

(9) "Covered entity" has the meaning given that term in 45 C.F.R. 160.103, as in effect on the effective date of this 2023 Act.

(10) "Decisions that produce legal effects or effects of similar significance" means decisions that result in providing or denying financial or lending services, housing, insurance, enrollment in education or educational opportunity, criminal justice, employment opportunities, health care services or access to essential goods and services.

(11) "Deidentified data" means data that:

(a) Cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable consumer, or to a device that identifies, is linked to or is reasonably linkable to a consumer; or

(b) Is:

(A) Derived from patient information that was originally created, collected, transmitted or maintained by an entity subject to regulation under the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as in effect on the effective date of this 2023 Act, or the Federal Policy for the Protection of Human Subjects, codified as 45 C.F.R. part 46 and in various other deferral regulations, as codified in various sections of the Code of Federal Regulations and as in effect on the effective date of this 2023 Act; and

(B) Deidentified as provided in 45 C.F.R. 164.514, as in effect on the effective date of this 2023 Act.

(12) "Device" means electronic equipment designed for a consumer's use that can transmit or receive personal data.

(13)(a) "Personal data" means data, derived data or any unique identifier that is linked to or is reasonably linkable to a consumer or to a device that identifies, is linked to or is reasonably linkable to one or more consumers in a household.

(b) "Personal data" does not include deidentified data or data that:

(A) Is lawfully available through federal, state or local government records or through widely distributed media; or

(B) A controller reasonably has understood to have been lawfully made available to the public by a consumer.

(14) "Process" or "processing" means an action, operation or set of actions or operations that is performed, automatically or otherwise, on personal data or on sets of personal data, such as collecting, using, storing, disclosing, analyzing, deleting or modifying the personal data.

(15) "Processor" means a person that processes personal data on behalf of a controller.

(16) "Profiling" means an automated processing of personal data for the purpose of evaluating, analyzing or predicting an identified or identifiable consumer's economic circumstances, health, personal preferences, interests, reliability, behavior, location or movements.

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

(b) "Sale" or "sell" does not include:

(A) A disclosure of personal data to a processor;

(B) A disclosure of personal data to an affiliate of a controller or to a third party for the purpose of enabling the controller to provide a product or service to a consumer that requested the product or service;

(C) A disclosure or transfer of personal data from a controller to a third party as part of a proposed or completed merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the controller's assets, including the personal data; or

(D) A disclosure of personal data that occurs because a consumer:

(i) Directs a controller to disclose the personal data;

(ii) Intentionally discloses the personal data in the course of directing a controller to interact with a third party; or

(iii) Intentionally discloses the personal data to the public by means of mass media, if the disclosure is not restricted to a specific audience.

(18)(a) "Sensitive data" means personal data that:

(A) Reveals a consumer's racial or ethnic background, national origin, religious beliefs, mental or physical condition or diagnosis, sexual orientation, status as transgender or nonbinary, status as a victim of crime or citizenship or immigration status;

(B) Is a child's personal data;

(C) Accurately identifies within a radius of 1,750 feet a consumer's present or past location, or the present or past location of a device that links or is linkable to a consumer by means of technology that includes, but is not limited to, a global positioning system that provides latitude and longitude coordinates; or

(D) Is genetic or biometric data.

(b) "Sensitive data" as defined in paragraph (a)(C) of this subsection 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.

(19)(a) "Targeted advertising" means advertising that is selected for display to a consumer on the basis of personal data obtained from the consumer's activities over time and across one or more unaffiliated websites or online applications and is used to predict the consumer's preferences or interests.

(b) "Targeted advertising" does not include:

(A) Advertisements that are based on activities within a controller's own websites or online applications;

(B) Advertisements based on the context of a consumer's current search query, visit to a specific website or use of an online application;

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

(D) A processing of personal data solely for the purpose of measuring or reporting an advertisement's frequency, performance or reach.

(20) "Third party" means a person, a public corporation, including the Oregon Health and Science University and the Oregon State Bar, or a public body, as defined in ORS 174.109, other than a consumer, a controller, a processor or an affiliate of a controller or processor.

SECTION 2. (1) Sections 1 to 9 of this 2023 Act apply to any person that conducts business in this state, or that provides products or services to residents of this state, and that during a calendar year, controls or processes:

(a) The personal data of 100,000 or more consumers, other than personal data controlled or processed solely for the purpose of completing a payment transaction; or

(b) The personal data of 25,000 or more consumers, while deriving 25 percent or more of the person's annual gross revenue from selling personal data.

(2) Sections 1 to 9 of this 2023 Act do not apply to:

(a) A public corporation, including the Oregon Health and Science University and the Oregon State Bar, or a public body, as defined in ORS 174.109;

(b) Protected health information that a covered entity or business associate processes in

accordance with, or documents that a covered entity or business associate creates for the purpose of complying with, the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, and regulations promulgated under the Act, as in effect on the effective date of this 2023 Act;

(c) Information used only for public health activities and purposes described in 45 C.F.R. 164.512, as in effect on the effective date of this 2023 Act;

(d) Information that identifies a consumer in connection with:

(A) Activities that are subject to the Federal Policy for the Protection of Human Subjects, codified as 45 C.F.R. part 46 and in various other federal regulations, as in effect on the effective date of this 2023 Act;

(B) Research on human subjects undertaken in accordance with good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(C) Activities that are subject to the protections provided in 21 C.F.R. parts 50 and 56, as in effect on the effective date of this 2023 Act; or

(D) Research conducted in accordance with the requirements set forth in subparagraphs (A) to (C) of this paragraph or otherwise in accordance with applicable law;

(e) Patient identifying information, as defined in 42 C.F.R. 2.11, as in effect on the effective date of this 2023 Act, that is collected and processed in accordance with 42 C.F.R. part 2;

(f) Patient safety work product, as defined in 42 C.F.R. 3.20, as in effect on the effective date of this 2023 Act, that is created for purposes of improving patient safety under 42 C.F.R. part 3;

(g) Information and documents created for the purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101 et seq., and implementing regulations, both as in effect on the effective date of this 2023 Act;

(h) Information that originates from, or that is intermingled so as to be indistinguishable from, information described in paragraphs (b) to (g) of this subsection that a covered entity or business associate, or a program of a qualified service organization, as defined in 42 C.F.R. 2.11, as in effect on the effective date of this 2023 Act, creates, collects, processes, uses or maintains in the same manner as is required under the laws, regulations and guidelines described in paragraphs (b) to (g) of this subsection;

(i) Information processed or maintained solely in connection with, and for the purpose of, enabling:

(A) An individual's employment or application for employment;

(B) An individual's ownership of, or function as a director or officer of, a business entity;

(C) An individual's contractual relationship with a business entity;

(D) An individual's receipt of benefits from an employer, including benefits for the individual's dependents or beneficiaries; or

(E) Notice of an emergency to persons that an individual specifies;

(j) Any activity that involves collecting, maintaining, disclosing, selling, communicating or using information for the purpose of evaluating a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living if done strictly in accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq., as in effect on the effective date of this 2023 Act, by:

(A) A consumer reporting agency, as defined in 15 U.S.C. 1681a(f), as in effect on the effective date of this 2023 Act;

(B) A person who furnishes information to a consumer reporting agency under 15 U.S.C. 1681s-2, as in effect on the effective date of this 2023 Act; or

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

(k) Information collected, processed, sold or disclosed under and in accordance with the following federal laws, all as in effect on the effective date of this 2023 Act:

(A) The Gramm-Leach-Bliley Act, P.L. 106-102, and regulations adopted to implement that Act;

(B) The Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq.;

(C) The Family Educational Rights and Privacy Act, 20 U.S.C. 1232g and regulations adopted to implement that Act; and

(D) The Airline Deregulation Act, P.L. 95-504, only to the extent that an air carrier collects information related to prices, routes or services and only to the extent that the provisions of the Airline Deregulation Act preempt sections 1 to 9 of this 2023 Act;

(L) A financial institution, as defined in ORS 706.008, or a financial institution's affiliate or subsidiary that is only and directly engaged in financial activities, as described in 12 U.S.C. 1843(k), as in effect on the effective date of this 2023 Act;

(m) Information that originates from, or is intermingled so as to be indistinguishable from, information described in paragraph (k)(A) of this subsection and that a licensee, as defined in ORS 725.010, collects, processes, uses or maintains in the same manner as is required under the laws and regulations specified in paragraph (k)(A) of this subsection;

(n) An insurer, as defined in ORS 731.106, other than a person that, alone or in combination with another person, establishes and maintains a self-insurance program and that does

not otherwise engage in the business of entering into policies of insurance;

(o) An insurance producer, as defined in ORS 731.104;

(p) An insurance consultant, as defined in ORS 744.602;

(q) A person that holds a third party administrator license issued under ORS 744.710;

(r) A nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance; and

(s) Noncommercial activity of:

(A) A publisher, editor, reporter or other person who is connected with or employed by a newspaper, magazine, periodical, newsletter, pamphlet, report or other publication in general circulation;

(B) A radio or television station that holds a license issued by the Federal Communications Commission;

(C) A nonprofit organization that provides programming to radio or television networks; or

(D) An entity that provides an information service, including a press association or wire service.

(3) Sections 1 to 9 of this 2023 Act do not prohibit a controller or processor from:

(a) Complying with federal, state or local statutes, ordinances, rules or regulations;

(b) Complying with a federal, state or local governmental inquiry, investigation, subpoena or summons related to a civil, criminal or administrative proceeding;

(c) Cooperating with a law enforcement agency concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or local statutes, ordinances, rules or regulations;

(d) Investigating, establishing, initiating or defending legal claims;

(e) Preventing, detecting, protecting against or responding to, and investigating, reporting or prosecuting persons responsible for, security incidents, identity theft, fraud, harassment or malicious, deceptive or illegal activity or preserving the integrity or security of systems;

(f) Identifying and repairing technical errors in a controller's or processor's information systems that impair existing or intended functionality;

(g) Providing a product or service that a consumer specifically requests from the controller or processor or requests as the parent or guardian of a child on the child's behalf or as the guardian or conservator of a person subject to a guardianship, conservatorship or other protective arrangement on the person's behalf;

(h) Negotiating, entering into or performing a contract with a consumer, including fulfilling the terms of a written warranty;

(i) Protecting any person's health and safety;

(j) Effectuating a product recall;

(k) Conducting internal research to develop, improve or repair products, services or technology;

(L) Performing internal operations that are reasonably aligned with a consumer's expectations, that the consumer may reasonably anticipate based on the consumer's existing relationship with the controller or that are otherwise compatible with processing data for the purpose of providing a product or service the consumer specifically requested or for the purpose of performing a contract to which the consumer is a party; or

(m) Assisting another controller or processor with any of the activities set forth in this subsection.

(4) Sections 1 to 9 of this 2023 Act do not apply to the extent that a controller's or processor's compliance with sections 1 to 9 of this 2023 Act would violate an evidentiary privilege under the laws of this state. Notwithstanding the provisions of sections 1 to 9 of this 2023 Act, a controller or processor may provide personal data about a consumer in a privileged communication to a person that is covered by an evidentiary privilege under the laws of this state.

(5) A controller may process personal data in accordance with subsection (3) of this section only to the extent that the processing is adequate and reasonably necessary for, relevant to, proportionate in relation to and limited to the purposes set forth in this section.

(6) Collection, use and retention of personal data under subsection (3)(e) and (f) of this section must, where applicable, take into account the nature and purpose of the collection, use or retention. The personal data must be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and security of the personal data and reduce reasonably foreseeable risks of harm to consumers from the collection, use or retention.

(7) A controller that claims that the controller's processing of personal data is exempt under subsection (3) of this section has the burden of demonstrating that the controller's processing qualifies for the exemption and complies with the requirements of subsections (5) and (6) of this section.

SECTION 3. (1) Subject to section 4 of this 2023 Act, a consumer may:

(a) Obtain from a controller:

(A) Confirmation as to whether the controller is processing or has processed the consumer's personal data and the categories of personal data the controller is processing or has processed;

(B) At the controller's option, a list of specific third parties, other than natural persons, to which the controller has disclosed:

(i) The consumer's personal data; or

(ii) Any personal data; and

(C) A copy of all of the consumer's personal data that the controller has processed or is processing;

(b) Require a controller to correct inaccuracies in personal data about the consumer, taking into account the nature of the personal data and the controller's purpose for processing the personal data;

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

(d) Opt out from a controller's processing of personal data of the consumer that the controller processes for any of the following purposes:

(A) Targeted advertising;

(B) Selling the personal data; or

(C) Profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance.

(2) A controller that provides a copy of personal data to a consumer under subsection (1)(a)(C) of this section shall provide the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal data to another person without hindrance.

(3) This section does not require a controller to disclose the controller's trade secrets, as defined in ORS 646.461.

SECTION 4. (1) A consumer may exercise the rights described in section 3 of this 2023 Act by submitting a request to a controller using the method that the controller specifies in the privacy notice described in section 5 of this 2023 Act.

(2) A controller may not require a consumer to create an account for the purpose described in subsection (1) of this section, but the controller may require the consumer to use an account the consumer created previously.

(3) A parent or legal guardian may exercise the rights described in section 3 of this 2023 Act on behalf of the parent's child or on behalf of a child for whom the guardian has legal responsibility. A guardian or conservator may exercise the rights described in subsection (1) of this section on behalf of a consumer that is subject to a guardianship, conservatorship or other protective arrangement.

(4) A consumer may designate another person to act on the consumer's behalf as the consumer's authorized agent for the purpose of opting out of a controller's processing of the consumer's personal data, as provided in section 3 (1)(d) of this 2023 Act. The consumer may designate an authorized agent by means of an internet link, browser setting, browser extension, global device setting or other technology that enables the consumer to opt out of the controller's processing of the consumer's personal data. A controller shall comply with an opt-out request the controller receives from an authorized agent if the controller can verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

(5) Except as otherwise provided in sections 1 to 9 of this 2023 Act, in responding to a request under subsection (1) of this section, a controller shall:

(a) Respond to a request from a consumer without undue delay and not later than 45 days after receiving the request. The controller may extend the period within which the controller responds by an additional 45 days if the extension is reasonably necessary to comply with the consumer's request, taking into consideration the complexity of the request and the number of requests the consumer makes. A controller that intends to extend the period for responding shall notify the consumer within the initial 45-day response period and explain the reason for the extension.

(b) Notify the consumer without undue delay and not later than 45 days after receiving the consumer's request if the controller declines to take action on the request. The controller in the notice shall explain the justification for not taking action and include instructions for appealing the controller's decision.

(c) Provide information the consumer requests once during any 12-month period without charge to the consumer. A controller may charge a reasonable fee to cover the administrative costs of complying with a second or subsequent request within the 12-month period, unless the purpose of the second or subsequent request is to verify that the controller corrected inaccuracies in, or deleted, the consumer's personal data in compliance with the consumer's request.

(d) Notify the consumer if the controller cannot, using commercially reasonable methods, authenticate the consumer's request without additional information from the consumer. A controller that sends a notification under this paragraph does not have to comply with the request until the consumer provides the information necessary to authenticate the request.

(e) Comply with a request under section 3 (1)(d) of this 2023 Act to opt out of the controller's processing of the consumer's personal data without requiring authentication, except that:

(A) A controller may ask for additional information necessary to comply with the request, such as information that is necessary to identify the consumer that requested to opt out.

(B) A controller may deny a request to opt out if the controller has a good-faith, reasonable and documented belief that the request is fraudulent. If the controller denies a request

under this subparagraph, the controller shall notify the consumer that the controller believes the request is fraudulent, stating in the notice that the controller will not comply with the request.

(6) A controller shall establish a process by means of which a consumer may appeal the controller's refusal to take action on a request under subsection (1) of this section. The controller's process must:

(a) Allow a reasonable period of time after the consumer receives the controller's refusal within which to appeal;

(b) Be conspicuously available to the consumer;

(c) Be similar to the manner in which a consumer must submit a request under subsection (1) of this section; and

(d) Require the controller to approve or deny the appeal within 45 days after the date on which the controller received the appeal and to notify the consumer in writing of the controller's decision and the reasons for the decision. If the controller denies the appeal, the notice must provide or specify information that enables the consumer to contact the Attorney General to submit a complaint.

(7) A controller that obtains personal data about a consumer from a source other than the consumer complies with the consumer's request to delete the personal data if the controller:

(a) Deletes the data but retains a record of the deletion request and a minimal amount of data necessary to ensure that the personal data remains deleted and does not use the minimal data for any other purpose; or

(b) Opts the consumer out of the controller's processing of the consumer's personal data for any purpose other than a purpose that is exempt under section 2 of this 2023 Act.

SECTION 5. (1) A controller shall:

(a) Specify in the privacy notice described in subsection (4) of this section the express purposes for which the controller is collecting and processing personal data;

(b) Limit the controller's collection of personal data to only the personal data that is adequate, relevant and reasonably necessary to serve the purposes the controller specified in paragraph (a) of this subsection;

(c) Establish, implement and maintain for personal data the same safeguards described in ORS 646A.622 that are required for protecting personal information, as defined in ORS 646A.602, such that the controller's safeguards protect the confidentiality, integrity and accessibility of the personal data to the extent appropriate for the volume and nature of the personal data; and

(d) Provide an effective means by which a consumer may revoke consent a consumer gave under sections 1 to 9 of this 2023 Act to the controller's processing of the consumer's personal data. The means must be at least as easy as the means by which the consumer provided consent. Once the consumer revokes consent, the controller shall cease processing the personal data as soon as is practicable, but not later than 15 days after receiving the revocation.

(2) A controller may not:

(a) Process personal data for purposes that are not reasonably necessary for and compatible with the purposes the controller specified in subsection (1)(a) of this section, unless the controller obtains the consumer's consent;

(b) Process sensitive data about a consumer without first obtaining the consumer's consent or, if the controller knows the consumer is a 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. and the regulations, rules and guidance adopted under the Act, all as in effect on the effective date of this 2023 Act;

(c) Process a consumer's personal data for the purposes of targeted advertising, of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance or of selling the consumer's personal data without the consumer's consent if the controller has actual knowledge that, or willfully disregards whether, the consumer is at least 13 years of age and not older than 15 years of age; or

(d) Discriminate against a consumer that exercises a right provided to the consumer under sections 1 to 9 of this 2023 Act by means such as denying goods or services, charging different prices or rates for goods or services or providing a different level of quality or selection of goods or services to the consumer.

(3) Subsections (1) and (2) of this section do not:

(a) Require a controller to provide a good or service that requires personal data from a consumer that the controller does not collect or maintain; or

(b) Prohibit a controller from offering a different price, rate, level of quality or selection of goods or services to a consumer, including an offer for no fee or charge, in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount or club card program.

(4) A controller shall provide to consumers a reasonably accessible, clear and meaningful privacy notice that:

(a) Lists the categories of personal data, including the categories of sensitive data, that the controller processes;

(b) Describes the controller's purposes for processing the personal data;

(c) Describes how a consumer may exercise the consumer's rights under sections 1 to 9 of this 2023 Act, including how a consumer may

appeal a controller's denial of a consumer's request under section 4 of this 2023 Act;

(d) Lists all categories of personal data, including the categories of sensitive data, that the controller shares with third parties;

(e) Describes all categories of third parties with which the controller shares personal data at a level of detail that enables the consumer to understand what type of entity each third party is and, to the extent possible, how each third party may process personal data;

(f) Specifies an electronic mail address or other online method by which a consumer can contact the controller that the controller actively monitors;

(g) Identifies the controller, including any business name under which the controller registered with the Secretary of State and any assumed business name that the controller uses in this state;

(h) Provides a clear and conspicuous description of any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance, and a procedure by which the consumer may opt out of this type of processing; and

(i) Describes the method or methods the controller has established for a consumer to submit a request under section 4 (1) of this 2023 Act.

(5) The method or methods described in subsection (4)(i) of this section for submitting a consumer's request to a controller must:

(a) Take into account:

(A) Ways in which consumers normally interact with the controller;

(B) A need for security and reliability in communications related to the request; and

(C) The controller's ability to authenticate the identity of the consumer that makes the request; and

(b) Provide a clear and conspicuous link to a webpage where the consumer or an authorized agent may opt out from a controller's processing of the consumer's personal data as described in section 3 (1)(d) of this 2023 Act or, solely if the controller does not have a capacity needed for linking to a webpage, provide another method the consumer can use to opt out.

(6) If a consumer or authorized agent uses a method described in subsection (5) of this section to opt out of a controller's processing of the consumer's personal data under section 3 (1)(d) of this 2023 Act and the decision conflicts with a consumer's voluntary participation in a bona fide reward, club card or loyalty program or a program that provides premium features or discounts in return for the consumer's consent to the controller's processing of the consumer's personal data, the controller may either comply with the request to opt out or notify the consumer of the conflict and ask the consumer to affirm that the consumer intends to withdraw from the bona fide reward, club card or loyalty program or the program that provides premium features or discounts. If the consumer affirms that the consumer intends to withdraw, the controller shall comply with the request to opt out.

SECTION 6. (1) A processor shall adhere to a controller's instructions and shall assist the controller in meeting the controller's obligations under sections 1 to 9 of this 2023 Act. In assisting the controller, the processor must:

(a) Enable the controller to respond to requests from consumers under section 4 of this 2023 Act by means that take into account how the processor processes personal data and the information available to the processor and that use appropriate technical and organizational measures to the extent reasonably practicable;

(b) Adopt administrative, technical and physical safeguards that are reasonably designed to protect the security and confidentiality of the personal data the processor processes, taking into account how the processor processes the personal data and the information available to the processor; and

(c) Provide information reasonably necessary for the controller to conduct and document data protection assessments.

(2) The processor shall enter into a contract with the controller that governs how the processor processes personal data on the controller's behalf. The contract must:

(a) Be valid and binding on both parties;

(b) Set forth clear instructions for processing data, the nature and purpose of the processing, the type of data that is subject to processing and the duration of the processing;

(c) Specify the rights and obligations of both parties with respect to the subject matter of the contract;

(d) Ensure that each person that processes personal data is subject to a duty of confidentiality with respect to the personal data;

(e) Require the processor to delete the personal data or return the personal data to the controller at the controller's direction or at the end of the provision of services, unless a law requires the processor to retain the personal data;

(f) Require the processor to make available to the controller, at the controller's request, all information the controller needs to verify that the processor has complied with all obligations the processor has under sections 1 to 9 of this 2023 Act;

(g) Require the processor to enter into a subcontract with a person the processor engages to assist with processing personal data on the controller's behalf and in the subcontract re-

quire the subcontractor to meet the processor's obligations under the processor's contract with the controller; and

(h) Allow the controller, the controller's designee or a qualified and independent person the processor engages, in accordance with an appropriate and accepted control standard, framework or procedure, to assess the processor's policies and technical and organizational measures for complying with the processor's obligations under sections 1 to 9 of this 2023 Act, and require the processor to cooperate with the assessment and, at the controller's request, report the results of the assessment to the controller.

(3) This section does not relieve a controller or processor from any liability that accrues under sections 1 to 9 of this 2023 Act as a result of the controller's or processor's actions in processing personal data.

(4)(a) For purposes of determining obligations under sections 1 to 9 of this 2023 Act, a person is a controller with respect to processing a set of personal data, and is subject to an action under section 9 of this 2023 Act to punish a violation of sections 1 to 9 of this 2023 Act, if the person:

(A) Does not need to adhere to another person's instructions to process the personal data;

(B) Does not adhere to another person's instructions with respect to processing the personal data when the person is obligated to do so; or

(C) Begins at any point to determine the purposes and means for processing the personal data, alone or in concert with another person.

(b) A determination under this subsection is a fact-based determination that must take account of the context in which a set of personal data is processed.

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

SECTION 7. (1)(a) A controller that possesses 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) Enter into a contract with a recipient of the deidentified data and provide in the contract that the recipient must comply with the controller's obligations under sections 1 to 9 of this 2023 Act.

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

(c) This section does not prohibit a controller from attempting to reidentify deidentified data solely for the purpose of testing the controller's methods for deidentifying data.

(2) Sections 1 to 9 of this 2023 Act do not:

(a) Require a controller or processor to:

(A) Reidentify deidentified data; or

(B) Associate a consumer with personal data in order to authenticate the consumer's request under section 4 of this 2023 Act by:

(i) Maintaining data in identifiable form; or

(ii) Collecting, retaining or accessing any particular data or technology.

(b) Require a controller or processor to comply with a consumer's request under section 4 of this 2023 Act if the controller:

(A) Cannot reasonably associate the request with personal data or if the controller's attempt to associate the request with personal data would be unreasonably burdensome;

(B) Does not use personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with any other personal data about the specific consumer; and

(C) Does not sell or otherwise voluntarily disclose personal data to a third party, except as otherwise provided in this section.

SECTION 8. (1)(a) 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.

(b) Processing activities that present a heightened risk of harm to a consumer include:

(A) Processing personal data for the purpose of targeted advertising;

(B) Processing sensitive data;

(C) Selling personal data; and

(D) Using the personal data for purposes of profiling, if 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) Physical or other types of intrusion upon a consumer's solitude, seclusion or private affairs or concerns, if the intrusion would be offensive to a reasonable person; or

(iv) Other substantial injury to consumers.

(c) A single data protection assessment may address a comparable set of processing operations that present a similar heightened risk of harm.

(2) A data protection assessment shall identify and weigh how processing personal data may directly or indirectly benefit the controller, the consumer, other stakeholders and the public against potential risks to the consumer, taking

into account how safeguards the controller employs can mitigate the risks. In conducting the assessment, the controller shall consider how deidentified data might reduce risks, the reasonable expectations of consumers, the context in which the data is processed and the relationship between the controller and the consumers whose personal data the controller will process.

(3) The Attorney General may require a controller to provide to the Attorney General any data protection assessments the controller has conducted if the data protection assessment is relevant to an investigation the Attorney General conducts under section 9 of this 2023 Act. The Attorney General may evaluate a data protection assessment for the controller's compliance with the requirements of sections 1 to 9 of this 2023 Act. If a data protection assessment the Attorney General obtains under this subsection includes information that is subject to attorney-client privilege or is work product that is subject to a privilege, the controller's provision of the data protection assessment does not waive the privilege.

(4) A data protection assessment that a controller conducts to comply with another applicable law or regulation satisfies the requirements of this section if the data protection assessment is reasonably similar in scope and effect to a data protection assessment conducted under this section.

(5) Requirements that apply to a data protection assessment under this section apply only to processing activities that occur on and after July 1, 2024, and are not retroactive.

(6) A controller shall retain for at least five years all data protection assessments the controller conducts under this section.

(7) A data protection assessment is confidential and is not subject to disclosure under ORS 192.311 to 192.478.

SECTION 9. (1)(a) The Attorney General may serve an investigative demand upon any person that possesses, controls or has custody of any information, document or other material that the Attorney General determines is relevant to an investigation of a violation of sections 1 to 9 of this 2023 Act or that could lead to a discovery of relevant information. An investigative demand may require the person to:

(A) Appear and testify under oath at the time and place specified in the investigative demand;

(B) Answer written interrogatories; or

(C) Produce relevant documents or physical evidence for examination at the time and place specified in the investigative demand.

(b) The Attorney General shall serve an investigative demand under this section in the manner provided in ORS 646.622. The Attorney General may enforce the investigative demand as provided in ORS 646.626.

(2)(a) An attorney may accompany, represent and advise in confidence a person that appears in response to a demand under subsection (1)(a)(A) of this section. The person may refuse to answer any question on constitutional grounds or on the basis of any other legal right or privilege, including protection against self-incrimination, but must answer any other question that is not subject to the right or privilege. If the person refuses to answer a question on grounds that the answer would be self-incriminating, the Attorney General may compel the person to testify as provided in ORS 136.617.

(b) The Attorney General shall exclude from the place in which the Attorney General conducts an examination under this subsection all persons other than the person the Attorney General is examining, the person's attorney, the officer before which the person gives the testimony and any stenographer recording the testimony.

(3)(a) The Attorney General shall hold in confidence and may not disclose to any person any documents, including data protection assessments, answers to interrogatories and transcripts of oral testimony, except that the Attorney General may disclose the documents to:

(A) The person that provided the documents or the oral testimony;

(B) The attorney or representative of the person that provided the documents or oral testimony;

(C) Employees of the Attorney General; or

(D) An official of the United States or of any state who is authorized to enforce federal or state consumer protection laws if the Attorney General first obtains a written agreement from the official in which the official agrees to abide by the confidentiality requirements of this subsection.

(b) The Attorney General may use any of the materials described in paragraph (a) of this subsection in any investigation the Attorney General conducts under this section or in any action or proceeding the Attorney General brings or initiates in a court or before an administrative agency in connection with the investigation.

(4)(a) The Attorney General may bring an action to seek a civil penalty of not more than $7,500 for each violation of sections 1 to 9 of this 2023 Act or to enjoin a violation or obtain other equitable relief. The Attorney General shall bring the action in the circuit court for Multnomah County or the circuit court of a county where any part of the violation occurred.

(b) A court may award reasonable attorney fees, expert witness fees and costs of investigation to the Attorney General if the Attorney General prevails in an action under this subsection. The court may award reasonable attorney

fees to a defendant that prevails in an action under this subsection if the court finds that the Attorney General had no objectively reasonable basis for asserting the claim or for appealing an adverse decision of the trial court.

(c) The Attorney General shall deposit the proceeds of any recovery under this subsection into the Department of Justice Protection and Education Revolving Account, as provided in ORS 180.095.

(5) Before bringing an action under subsection (4) of this section, the Attorney General shall notify a controller of a violation of sections 1 to 9 of this 2023 Act if the Attorney General determines that the controller can cure the violation. If the controller fails to cure the violation within 30 days after receiving the notice of the violation, the Attorney General may bring the action without further notice.

(6) The Attorney General shall bring an action under subsection (4) of this section within five years after the date of the last act of a controller that constituted the violation for which the Attorney General seeks relief.

(7) The remedies available to the Attorney General under subsection (4) of this section are in addition to and not in lieu of any other relief available to the Attorney General or another person under other applicable provisions of law. A claim available under another provision of law may be joined to the Attorney General's claim under subsection (4) of this section.

(8) The Attorney General has exclusive authority to enforce the provisions of sections 1 to 9 of this 2023 Act. Sections 1 to 9 of this 2023 Act, or any other laws of this state, do not create a private right of action to enforce a violation of sections 1 to 9 of this 2023 Act.

SECTION 10. ORS 180.095 is amended to read:

180.095. (1) The Department of Justice Protection and Education Revolving Account is created in the General Fund. All moneys in the account are continuously appropriated to the Department of Justice and may be used to pay for only the following activities:

(a) Restitution and refunds in proceedings described in paragraph (c) of this subsection;

(b) Consumer and business education relating to the laws governing antitrust and unlawful trade practices; and

(c) Personal services, travel, meals, lodging and all other costs and expenses incurred by the department in investigating, preparing, commencing and prosecuting the following actions and suits, and enforcing judgments, settlements, compromises and assurances of voluntary compliance arising out of the following actions and suits:

(A) Actions and suits under the state and federal antitrust laws;

(B) Actions and suits under ORS 336.184 and 646.605 to 646.656;

(C) Actions commenced under ORS 59.331; [*and*]

(D) Actions and suits under ORS 180.750 to 180.785[.]**; and**

(E) Actions commenced under section 9 of this 2023 Act.

(2) Moneys in the Department of Justice Protection and Education Revolving Account are not subject to allotment. Upon request of the Attorney General, the State Treasurer shall create subaccounts within the account for the purposes of managing moneys in the account and allocating those moneys to the activities described in subsection (1) of this section.

(3) Except as otherwise provided by law, all sums of money received by the Department of Justice under a judgment, settlement, compromise or assurance of voluntary compliance, including damages, restitution, refunds, attorney fees, costs, disbursements and other recoveries, but excluding civil penalties under ORS 646.642, in proceedings described in subsection (1)(c) of this section shall, upon receipt, be deposited with the State Treasurer to the credit of the Department of Justice Protection and Education Revolving Account. However, if the action or suit was based on an expenditure or loss from a public body or a dedicated fund, the amount of such expenditure or loss, after deduction of attorney fees and expenses awarded to the department by the court or agreed to by the parties, if any, shall be credited to the public body or dedicated fund and the remainder thereof credited to the Department of Justice Protection and Education Revolving Account.

(4) If the Department of Justice recovers restitution or refunds in a proceeding described in subsection (1)(c) of this section, and the department cannot determine the persons to whom the restitution or refunds should be paid or the amount of the restitution or refund payable to individual claimants is de minimis, the restitution or refunds may not be deposited in the Department of Justice Protection and Education Revolving Account and shall be deposited in the General Fund.

(5) Before April 1 of each odd-numbered year, the Department of Justice shall report to the Joint Committee on Ways and Means:

(a) The department's projection of the balance in the Department of Justice Protection and Education Revolving Account at the end of the biennium in which the report is made and at the end of the following biennium;

(b) The amount of the balance held for restitution and refunds;

(c) An estimate of the department's anticipated costs and expenses under subsection (1)(b) and (c) of this section for the biennium in which the report is made and for the following biennium; and

(d) Any judgment, settlement, compromise or other recovery, the proceeds of which are used for purposes other than:

(A) For deposit into the Department of Justice Protection and Education Revolving Account; or

(B) For payment of legal costs related to the judgment, settlement, compromise or other recovery.

(6) The Joint Committee on Ways and Means, after consideration of recommendations made by the Department of Justice, shall use the information reported under subsection (5) of this section to determine an appropriate balance for the revolving account.

SECTION 11. Section 9 of this 2023 Act is amended to read:

Sec. 9. (1)(a) The Attorney General may serve an investigative demand upon any person that possesses, controls or has custody of any information, document or other material that the Attorney General determines is relevant to an investigation of a violation of sections 1 to 9 of this 2023 Act or that could lead to a discovery of relevant information. An investigative demand may require the person to:

(A) Appear and testify under oath at the time and place specified in the investigative demand;

(B) Answer written interrogatories; or

(C) Produce relevant documents or physical evidence for examination at the time and place specified in the investigative demand.

(b) The Attorney General shall serve an investigative demand under this section in the manner provided in ORS 646.622. The Attorney General may enforce the investigative demand as provided in ORS 646.626.

(2)(a) An attorney may accompany, represent and advise in confidence a person that appears in response to a demand under subsection (1)(a)(A) of this section. The person may refuse to answer any question on constitutional grounds or on the basis of any other legal right or privilege, including protection against self-incrimination, but must answer any other question that is not subject to the right or privilege. If the person refuses to answer a question on grounds that the answer would be self-incriminating, the Attorney General may compel the person to testify as provided in ORS 136.617.

(b) The Attorney General shall exclude from the place in which the Attorney General conducts an examination under this subsection all persons other than the person the Attorney General is examining, the person's attorney, the officer before which the person gives the testimony and any stenographer recording the testimony.

(3)(a) The Attorney General shall hold in confidence and may not disclose to any person any documents, including data protection assessments, answers to interrogatories and transcripts of oral testimony, except that the Attorney General may disclose the documents to:

(A) The person that provided the documents or the oral testimony;

(B) The attorney or representative of the person that provided the documents or oral testimony;

(C) Employees of the Attorney General; or

(D) An official of the United States or of any state who is authorized to enforce federal or state consumer protection laws if the Attorney General first obtains a written agreement from the official in which the official agrees to abide by the confidentiality requirements of this subsection.

(b) The Attorney General may use any of the materials described in paragraph (a) of this subsection in any investigation the Attorney General conducts under this section or in any action or proceeding the Attorney General brings or initiates in a court or before an administrative agency in connection with the investigation.

(4)(a) The Attorney General may bring an action to seek a civil penalty of not more than $7,500 for each violation of sections 1 to 9 of this 2023 Act or to enjoin a violation or obtain other equitable relief. The Attorney General shall bring the action in the circuit court for Multnomah County or the circuit court of a county where any part of the violation occurred.

(b) A court may award reasonable attorney fees, expert witness fees and costs of investigation to the Attorney General if the Attorney General prevails in an action under this subsection. The court may award reasonable attorney fees to a defendant that prevails in an action under this subsection if the court finds that the Attorney General had no objectively reasonable basis for asserting the claim or for appealing an adverse decision of the trial court.

(c) The Attorney General shall deposit the proceeds of any recovery under this subsection into the Department of Justice Protection and Education Revolving Account, as provided in ORS 180.095.

[*(5) Before bringing an action under subsection (4) of this section, the Attorney General shall notify a controller of a violation of sections 1 to 9 of this 2023 Act if the Attorney General determines that the controller can cure the violation. If the controller fails to cure the violation within 30 days after receiving the notice of the violation, the Attorney General may bring the action without further notice.*]

[*(6)*] **(5)** The Attorney General shall bring an action under subsection (4) of this section within five years after the date of the last act of a controller that constituted the violation for which the Attorney General seeks relief.

[*(7)*] **(6)** The remedies available to the Attorney General under subsection (4) of this section are in addition to and not in lieu of any other relief available to the Attorney General or another person under other applicable provisions of law. A claim available under another provision of law may be joined to the Attorney General's claim under subsection (4) of this section.

[*(8)*] **(7)** The Attorney General has exclusive authority to enforce the provisions of sections 1 to 9 of this 2023 Act. Sections 1 to 9 of this 2023 Act, or any other laws of this state, do not create a private right of action to enforce a violation of sections 1 to 9 of this 2023 Act.

SECTION 12. Section 5 of this 2023 Act is amended to read:

Sec. 5. (1) A controller shall:

(a) Specify in the privacy notice described in subsection (4) of this section the express purposes

for which the controller is collecting and processing personal data;

(b) Limit the controller's collection of personal data to only the personal data that is adequate, relevant and reasonably necessary to serve the purposes the controller specified in paragraph (a) of this subsection;

(c) Establish, implement and maintain for personal data the same safeguards described in ORS 646A.622 that are required for protecting personal information, as defined in ORS 646A.602, such that the controller's safeguards protect the confidentiality, integrity and accessibility of the personal data to the extent appropriate for the volume and nature of the personal data; and

(d) Provide an effective means by which a consumer may revoke consent a consumer gave under sections 1 to 9 of this 2023 Act to the controller's processing of the consumer's personal data. The means must be at least as easy as the means by which the consumer provided consent. Once the consumer revokes consent, the controller shall cease processing the personal data as soon as is practicable, but not later than 15 days after receiving the revocation.

(2) A controller may not:

(a) Process personal data for purposes that are not reasonably necessary for and compatible with the purposes the controller specified in subsection (1)(a) of this section, unless the controller obtains the consumer's consent;

(b) Process sensitive data about a consumer without first obtaining the consumer's consent or, if the controller knows the consumer is a 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. and the regulations, rules and guidance adopted under the Act, all as in effect on the effective date of this 2023 Act;

(c) Process a consumer's personal data for the purposes of targeted advertising, of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance or of selling the consumer's personal data without the consumer's consent if the controller has actual knowledge that, or willfully disregards whether, the consumer is at least 13 years of age and not older than 15 years of age; or

(d) Discriminate against a consumer that exercises a right provided to the consumer under sections 1 to 9 of this 2023 Act by means such as denying goods or services, charging different prices or rates for goods or services or providing a different level of quality or selection of goods or services to the consumer.

(3) Subsections (1) and (2) of this section do not:

(a) Require a controller to provide a good or service that requires personal data from a consumer that the controller does not collect or maintain; or

(b) Prohibit a controller from offering a different price, rate, level of quality or selection of goods or services to a consumer, including an offer for no fee or charge, in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount or club card program.

(4) A controller shall provide to consumers a reasonably accessible, clear and meaningful privacy notice that:

(a) Lists the categories of personal data, including the categories of sensitive data, that the controller processes;

(b) Describes the controller's purposes for processing the personal data;

(c) Describes how a consumer may exercise the consumer's rights under sections 1 to 9 of this 2023 Act, including how a consumer may appeal a controller's denial of a consumer's request under section 4 of this 2023 Act;

(d) Lists all categories of personal data, including the categories of sensitive data, that the controller shares with third parties;

(e) Describes all categories of third parties with which the controller shares personal data at a level of detail that enables the consumer to understand what type of entity each third party is and, to the extent possible, how each third party may process personal data;

(f) Specifies an electronic mail address or other online method by which a consumer can contact the controller that the controller actively monitors;

(g) Identifies the controller, including any business name under which the controller registered with the Secretary of State and any assumed business name that the controller uses in this state;

(h) Provides a clear and conspicuous description of any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance, and a procedure by which the consumer may opt out of this type of processing; and

(i) Describes the method or methods the controller has established for a consumer to submit a request under section 4 (1) of this 2023 Act.

(5) The method or methods described in subsection (4)(i) of this section for submitting a consumer's request to a controller must:

(a) Take into account:

(A) Ways in which consumers normally interact with the controller;

(B) A need for security and reliability in communications related to the request; and

(C) The controller's ability to authenticate the identity of the consumer that makes the request; [*and*]

(b) Provide a clear and conspicuous link to a webpage where the consumer or an authorized agent may opt out from a controller's processing of the consumer's personal data as described in section 3 (1)(d) of this 2023 Act or, solely if the controller does not have a capacity needed for linking to a webpage, provide another method the consumer can use to opt out[.]**; and**

(c) Allow a consumer or authorized agent to send a signal to the controller that indicates the

consumer's preference to opt out of the sale of personal data or targeted advertising under section 3 (1)(d) of this 2023 Act by means of a platform, technology or mechanism that:

(A) Does not unfairly disadvantage another controller;

(B) Does not use a default setting but instead requires the consumer or authorized agent to make an affirmative, voluntary and unambiguous choice to opt out;

(C) Is consumer friendly and easy for an average consumer to use;

(D) Is as consistent as possible with similar platforms, technologies or mechanisms required under federal or state laws or regulations; and

(E) Enables the controller to accurately determine whether the consumer is a resident of this state and has made a legitimate request under section 4 of this 2023 Act to opt out as described in section 3 (1)(d) of this 2023 Act.

(6) If a consumer or authorized agent uses a method described in subsection (5) of this section to opt out of a controller's processing of the consumer's personal data under section 3 (1)(d) of this 2023 Act and the decision conflicts with a consumer's voluntary participation in a bona fide reward, club card or loyalty program or a program that provides premium features or discounts in return for the consumer's consent to the controller's processing of the consumer's personal data, the controller may either comply with the request to opt out or notify the consumer of the conflict and ask the consumer to affirm that the consumer intends to withdraw from the bona fide reward, club card or loyalty program or the program that provides premium features or discounts. If the consumer affirms that the consumer intends to withdraw, the controller shall comply with the request to opt out.

SECTION 13. Sections 1 to 9 of this 2023 Act do not apply before July 1, 2025, to the activities of an organization described in section 501(c)(3) of the Internal Revenue Code that is exempt from income tax under section 501(a) of the Internal Revenue Code.

SECTION 14. Notwithstanding any other law limiting expenditures, the limitation on expenditures established by section 2 (3), chapter 382, Oregon Laws 2023 (Enrolled Senate Bill 5514), for the biennium beginning July 1, 2023, as the maximum limit for payment of expenses from fees, moneys or other revenues, including Miscellaneous Receipts, but excluding lottery funds and federal funds, collected or received by the Department of Justice for the Civil Enforcement Division, is increased by $1,780,729 for the purpose of carrying out the provisions of this 2023 Act.

SECTION 15. (1) Sections 1 to 9 of this 2023 Act and the amendments to ORS 180.095 by section 10 of this 2023 Act become operative on July 1, 2024.

(2) The amendments to section 5 of this 2023 Act by section 12 of this 2023 Act become operative on January 1, 2026.

(3) The amendments to section 9 of this 2023 Act by section 11 of this 2023 Act become operative on January 1, 2026.

Approved by the Governor July 18, 2023
Filed in the office of Secretary of State July 18, 2023
Effective date January 1, 2024