83rd OREGON LEGISLATIVE ASSEMBLY--2025 Regular Session

House Bill 3899

Sponsored by Representatives CHOTZEN, PHAM H, Senator BROADMAN; Representatives DOBSON, FRAGALA, GOMBERG, MANNIX, SKARLATOS, SOSA, WALTERS, Senators CAMPOS, GOLDEN, PHAM K

SUMMARY

The following summary is not prepared by the sponsors of the measure and is not a part of the body thereof subject to consideration by the Legislative Assembly. It is an editor's brief statement of the essential features of the measure **as introduced.** The statement includes a measure digest written in compliance with applicable readability standards.

Digest: Changes some of the laws that apply to the use of personal data of consumers. (Flesch Readability Score: 67.5).

Lowers the thresholds above which, in applicable circumstances, controllers are subject to regulation in processing consumers' personal data. Prohibits controllers from processing sensitive data for the purposes of targeted advertising or profiling a consumer in furtherance of decisions that produce legal effects or effects of similar significance. Prohibits a controller from selling sensitive data for any reason.

A BILL FOR AN ACT

Relating to requirements that apply to persons that process consumer personal data; amending ORS 646A.572 and 646A.578.

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

SECTION 1. ORS 646A.572 is amended to read:

646A.572. (1) ORS 646A.570 to 646A.589 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*] **35,000** 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*] **10,000** or more consumers, while deriving [*25*] **20** percent or more of the person's annual gross revenue from selling personal data.

(2) ORS 646A.570 to 646A.589 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 January 1, 2024;

(c) Information used only for public health activities and purposes described in 45 C.F.R. 164.512, as in effect on January 1, 2024;

(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 January 1, 2024;

(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;

NOTE: Matter in **boldfaced** type in an amended section is new; matter [*italic and bracketed*] is existing law to be omitted. New sections are in **boldfaced** type.

(C) Activities that are subject to the protections provided in 21 C.F.R. parts 50 and 56, as in effect on January 1, 2024; 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 January 1, 2024, 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 January 1, 2024, 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 January 1, 2024;

(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 January 1, 2024, 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 January 1, 2024, by:

(A) A consumer reporting agency, as defined in 15 U.S.C. 1681a(f), as in effect on January 1, 2024;

(B) A person who furnishes information to a consumer reporting agency under 15 U.S.C. 1681s-2, as in effect on January 1, 2024; 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 January 1, 2024:

(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 ORS 646A.570 to 646A.589;

(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 January 1, 2024;

(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) ORS 646A.570 to 646A.589 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) ORS 646A.570 to 646A.589 do not apply to the extent that a controller's or processor's compliance with ORS 646A.570 to 646A.589 would violate an evidentiary privilege under the laws of this state. Notwithstanding the provisions of ORS 646A.570 to 646A.589, 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 2. ORS 646A.578, as amended by section 12, chapter 369, Oregon Laws 2023, is amended to read:

646A.578. (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 ORS 646A.570 to 646A.589 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 January 1, 2024;

(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) Process sensitive data for the purposes of targeted advertising or for the purpose of profiling a consumer in furtherance of decisions that produce legal effects or effects of similar significance, whether the controller has the consumer's consent or not;

(e) Sell sensitive data for any reason, with or without a consumer's consent; or

[*(d)*] **(f)** Discriminate against a consumer that exercises a right provided to the consumer under ORS 646A.570 to 646A.589 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 ORS 646A.570 to 646A.589, including how a consumer may appeal a controller's denial of a consumer's request under ORS 646A.576;

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

(e) States that the controller may not sell sensitive data for any reason and may not process sensitive data for the purposes of targeted advertising or for the purpose of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance;

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

[*(g)*] **(h)** 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)*] **(i)** 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)*] **(j)** Describes the method or methods the controller has established for a consumer to submit a request under ORS 646A.576 (1).

(5) The method or methods described in subsection [*(4)(i)*] **(4)(j)** 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;

(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 ORS 646A.574 (1)(d) 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 ORS 646A.574 (1)(d) 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 ORS 646A.576 to opt out as described in ORS 646A.574 (1)(d).

(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 ORS 646A.574 (1)(d) 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.