H-1444.1

SUBSTITUTE HOUSE BILL 1671

State of Washington 69th Legislature 2025 Regular Session

By House Technology, Economic Development, & Veterans (originally sponsored by Representatives Kloba, Fosse, Doglio, Parshley, Berry, Ramel, Scott, Taylor, and Simmons)

READ FIRST TIME 02/18/25.

AN ACT Relating to personal data privacy; adding a new section to chapter 19.373 RCW; adding a new chapter to Title 19 RCW; creating a new section; providing an effective date; and providing an expiration date.

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

NEW SECTION. **Sec. 1.** DEFINITIONS. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Affiliate" has the same meaning as defined in RCW 19.373.010.

(2)(a) "Affirmative consent" or "consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, revokable, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a controller, provided that:

(i) The request is provided to the consumer in a clear and conspicuous stand-alone disclosure;

(ii) The request includes a description of the processing purpose for which the consumer's consent is sought and (A) clearly distinguishes between an act or practice that is necessary to fulfill a request of the consumer and an act or practice that is for another

purpose, (B) clearly states the specific categories of personal data that the controller intends to collect, process, or transfer under each act or practice, and (C) is written in easy to understand language and includes a prominent heading that would enable a reasonable consumer to identify and understand each act or practice;

(iii) The request clearly explains the consumer's rights related to consent;

(iv) The request is made in a manner reasonably accessible to and usable by consumers with disabilities;

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

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

(vii) Affirmative consent to an act or practice is not inferred from the inaction of the consumer or the consumer's continued use of a service or product provided by the controller.

(b) "Affirmative consent" does not include:

(i) Acceptance of a general or broad terms 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;

(iii) Agreement obtained through the use of a false, fraudulent, or materially misleading statement or representation; or

(iv) Agreement obtained through the use of dark patterns.

(3) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded in this chapter is being made by, or on behalf of, the consumer who is entitled to exercise such rights with respect to the personal data at issue.

(4) "Biometric data" has the same meaning as defined in RCW 19.373.010.

(5) "Child" means a consumer under the age of 13 years old.

(6) "Collect" means buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring personal data by any means.

(7) "Consumer" means a natural person who is a Washington resident and who acts only in an individual or household context, however identified, including by any unique identifier. The location

of a person in Washington state creates a presumption that the person is a Washington resident. "Consumer" does not include an individual acting in an employment context.

(8)(a) "Consumer health data" means personal data that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status.

(b) For the purposes of this definition, physical or mental health status includes, but is not limited to:

(i) Individual health conditions, treatment, diseases, or diagnosis;

(ii) Social, psychological, behavioral, and medical interventions;

(iii) Health-related surgeries or procedures;

(iv) Use or purchase of prescribed medication;

(v) Bodily functions, vital signs, symptoms, or measurements of such information;

(vi) Diagnoses or diagnostic testing, treatment, or medication;

(vii) Gender-affirming care information;

(viii) Reproductive or sexual health information;

(ix) Biometric data;

(x) Genetic data;

(xi) Precise geolocation information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;

(xii) Data that identifies a consumer seeking health care services; or

(xiii) Any information that a controller or processor processes to associate or identify a consumer with the data described in (b)(i) through (xii) of this subsection that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

(c) "Consumer health data" does not include personal data that is used to engage in public or peer-reviewed scientific, historical, 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, human subjects research ethics review board, or a similar independent oversight entity that determines that the controller or processor has implemented

reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

(9)(a) "Contextual advertising" means displaying or presenting an advertisement that does not vary based on the identity of the individual recipient and is based solely on the immediate content of a web page or online service within which the advertisement appears, or on a specific request of the consumer for information or feedback, if displayed in proximity to the results of such request for information.

(b) A controller may use the following types of personal data to display a contextual advertisement, provided that the personal data is not used to make inferences about the consumer, profile the consumer, or for any other purpose, and that the consumer may use technical means to obfuscate or change the consumer's physical location and specify a language preference:

(i) Technical specifications that are necessary for the ad to be delivered and displayed properly on a given device;

(ii) A consumer's immediate presence in a geographic area with a radius no smaller than 10 miles, or an area reasonably estimated to include online activity from at least 5,000 users, but not including precise geolocation data; or

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

(10) "Controller" means the natural or legal person who, alone or jointly with others, determines the purposes and means of collecting or processing of personal data.

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

(12) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions that result in access to, or the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to essential goods or services.

(13) "Deidentified data" means data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses the data:

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

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

(c) Contractually obligates any recipients of the data to comply with (a) and (b) of this subsection.

(14) "First party" means a consumer-facing controller with which the consumer intends or expects to interact.

(15)(a) "First-party advertising" means processing by a first party of its own first-party data for the purposes of advertising and marketing and is carried out:

(i) Through direct communications with a consumer, such as direct mail, email, or text message communications;

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

(iii) Through display or presentation of an advertisement on the first party's own website, application, or its other online content.

(b) "First-party advertising" includes marketing measurement related to such advertising and marketing.

(16) "First-party data" means personal data collected directly from a consumer by a first party, including based on a visit by the consumer to or use by the consumer of a website, a physical location, or an online service operated by the first party.

(17) "Gender-affirming care information" means personal data relating to seeking or obtaining past, present, or future gender-affirming care services. "Gender-affirming care information" includes, but is not limited to:

(a) Precise geolocation information that could reasonably indicate a consumer's attempt to acquire or receive gender-affirming care services;

(b) Efforts to research or obtain gender-affirming care services; or

(c) Any gender-affirming care information that is derived, extrapolated, or inferred, including from nonhealth information, such as proxy, derivative, inferred, emergent, or algorithmic data.

(18) "Gender-affirming care services" has the same meaning as in RCW 19.373.010.

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

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

(21) "Minor" means any consumer who is younger than 18 years of age.

(22) "Person" means an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust, or any other legal entity.

(23) "Personal data" means any information that identifies or is reasonably capable of being associated or linked, directly or indirectly, with a particular consumer. "Personal data" includes, but is not limited to, derived data and data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier. "Personal data" does not include publicly available information or deidentified data.

(24)(a) "Precise geolocation data" means information derived from technology including, but not limited to, latitude and longitude coordinates from global positioning system mechanisms or other similar positional data, that reveals the past or present physical location of an individual or device that identifies or is linked or reasonably linkable to one or more individuals with precision and accuracy within a radius of 1,750 feet.

(b) "Precise geolocation information" does not include the content of communications, a photograph or video, metadata associated with a photograph or video that cannot be linked to an individual, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(25) "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 use, storage, disclosure, analysis, deletion, or modification of personal data.

(26) "Processor" means a person that collects, processes, or transfers personal data on behalf of, and at the direction of, a controller or another processor.

(27) "Profiling" means any form of processing performed on personal data to evaluate, analyze, or predict personal aspects, including an individual's economic situation, health, personal

preferences, interests, reliability, behavior, location, or movements.

(28)(a) "Publicly available information" means information that has been lawfully made available to the general public from:

(i) Federal, state, or municipal government records, if the person collects, processes, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity;

(ii) Widely distributed media; or

(iii) A disclosure to the general public as required by federal, state, or local law.

(b) "Publicly available information" does not include:

(i) Any obscene visual depiction, as defined in 18 U.S.C. Sec. 1460;

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

(iii) Biometric data;

(iv) Personal data that is created through the combination of personal data with publicly available information;

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

(vi) Information made available by a consumer on a website or online service made available to all members of the public, for free or for a fee, where the consumer has restricted the information to a specific audience; or

(vii) Intimate images and fabricated intimate images disclosed without consent of the depicted individual. For the purposes of this subsection, "intimate image," "fabricated intimate image," and "depicted individual" have the same meaning as defined in RCW 7.110.010.

(29) "Reproductive or sexual health information" means personal data relating to seeking or obtaining past, present, or future reproductive or sexual health services. "Reproductive or sexual health information" includes, but is not limited to:

(a) Precise geolocation information that could reasonably indicate a consumer's attempt to acquire or receive reproductive or sexual health services;

(b) Efforts to research or obtain reproductive or sexual health services; or

(c) Any reproductive or sexual health information that is derived, extrapolated, or inferred, including from nonhealth information, such as proxy, derivative, inferred, emergent, or algorithmic data.

(30) "Reproductive or sexual health services" has the same meaning as defined in RCW 19.373.010.

(31)(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) "Sale of personal data" 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 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) With the consumer's affirmative consent, the disclosure of personal data where the consumer affirmatively directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party; or

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

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

(a) Data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, status as pregnant, sex life, sexual orientation, status as transgender or nonbinary, union membership, income level or indebtedness, or citizenship or immigration status;

(b) Consumer health data;

(c) Genetic or biometric data;

(d) Personal data of a consumer that a controller knows, or willfully disregards, is a minor;

(e) Precise geolocation data;

(f) A government-issued identifier, including a social security number, passport number, or driver's license number, that is not required by law to be displayed in public; or

(g) The online activities of a consumer or device linked or reasonably linkable to a consumer over time and across websites,

online applications, or mobile applications that do not share common branding, or data generated by profiling performed on such data.

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

(b) "Targeted advertising" includes displaying or presenting an online advertisement for a product or service based on the previous interaction of a consumer or a device identified by a unique persistent identifier with such product or service on a website or online service that does not share common branding with the website or online service displaying or presenting the advertisement, and marketing measurement related to such advertisements.

(c) "Targeted advertising" does not include first-party advertising or contextual advertising.

(34) "Third party" means a person that collects personal data from another person that is not the consumer to whom the data pertains and is not a processor with respect to such data. "Third party" does not include a person that collects personal data from another entity if the two entities are affiliates.

(35) "Transfer" means to disclose, release, disseminate, make available, license, rent, or share personal data to a third party orally, in writing, electronically, or by any other means.

(36)(a) "Unique persistent identifier" means a technologically created identifier to the extent that such identifier is reasonably linkable to a consumer or a device that identifies or is linked or reasonably linkable to one or more consumers.

(b) "Unique persistent identifier" includes device identifiers, internet protocol addresses, cookies, beacons, pixel tags, mobile ad identifiers or similar technology customer numbers, unique pseudonyms, user aliases, telephone numbers, or other forms of persistent or probabilistic identifiers that are linked or reasonably linkable to one or more consumers or devices.

(c) "Unique persistent identifier" does not include an identifier assigned by a controller for the sole purpose of giving effect to the exercise of affirmative consent or opt out by a consumer with respect

to the collecting, processing, and transfer of personal data, or with respect to otherwise limiting the collecting, processing, or transfer of personal data.

NEW SECTION. **Sec. 2.** APPLICABILITY AND SCOPE. (1) This chapter applies to persons that conduct business in Washington state or produce products or services that are targeted to residents of Washington state, and that collect or process the personal data of consumers.

(2) This chapter does not apply to any federal, state, tribal, territorial, or local government entity, such as a body, authority, board, bureau, commission, district, or agency, of this state or of any political subdivision of this state, or a contracted service provider when processing personal data on behalf of a government entity.

(3) This chapter does not apply to the following information and data:

(a) Protected health information that a covered entity or business associate collects or processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with, the federal health insurance portability and accountability act of 1996 and its implementing regulations;

(b) Health care information collected, used, or disclosed in accordance with chapter 70.02 RCW;

(c) Patient identifying information as defined by 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

(d) Identifiable private information for purposes of: The federal policy for the protection of human subjects under 45 C.F.R. Part 46, 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 harmonization of technical requirements for pharmaceuticals for human use, the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, personal data used or shared in research as defined in 45 C.F.R. 164.501 that is conducted in accordance with one or more of the requirements set forth in this subsection, or other research conducted in accordance with applicable law;

(e) Information and documents created specifically for, and collected and maintained by:

(i) A quality improvement committee for purposes of RCW 43.70.510, 70.230.080, or 70.41.200;

(ii) A peer review committee for purposes of RCW 4.24.250;

(iii) A quality assurance committee for purposes of RCW 74.42.640 or 18.20.390;

(iv) A hospital, as defined in RCW 43.70.056, for reporting of health care-associated infections for purposes of RCW 43.70.056, a notification of an incident for purposes of RCW 70.56.040(5), or reports regarding adverse events for purposes of RCW 70.56.020(2)(b); or

(v) A manufacturer, as defined in 21 C.F.R. Sec. 820.3(o), when collected, used, or disclosed for purposes specified in chapter 70.02 RCW;

(f) Information and documents created for purposes of the federal health care quality improvement act of 1986, and related regulations;

(g) Patient safety work product for purposes of the federal patient safety and quality improvement act, 42 U.S.C. Sec. 299b-21 et seq.;

(h) Information that is deidentified in accordance with the requirements for deidentification set forth in 45 C.F.R. Part 164 and derived from any of the health care-related information identified in this subsection;

(i) Information originating from, and intermingled so as to be indistinguishable with, information described in (a) through (h) of this subsection that is maintained by:

(i) A covered entity or business associate as defined by the health insurance portability and accountability act of 1996 and related regulations;

(ii) A health care facility or health care provider as defined in RCW 70.02.010; or

(iii) A program or a qualified service organization as defined by 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

(j) Information used only for public health activities and purposes as described in 45 C.F.R. Sec. 164.512 or that is part of a limited data set, as defined, and is used, disclosed, and maintained in the manner required, by 45 C.F.R. Sec. 164.514;

(k) Identifiable data collected, used, or disclosed in accordance with chapter 43.371 RCW or RCW 69.43.165;

(l) Personal information that is governed by and collected, processed, sold, or disclosed pursuant to the following regulations, parts, titles, or acts:

(i) The Gramm-Leach-Bliley act, 15 U.S.C. Sec. 6801 et seq., and implementing regulations;

(ii) Part C of Title XI of the social security act, 42 U.S.C. Sec. 1320d et seq.;

(iii) The fair credit reporting act, 15 U.S.C. Sec. 1681 et seq.;

(iv) The family educational rights and privacy act, 20 U.S.C. 1232g; 34 C.F.R. Part 99;

(v) The Washington health benefit exchange and applicable statutes and regulations, including 45 C.F.R. Sec. 155.260 and chapter 43.71 RCW;

(vi) Privacy rules adopted by the office of the insurance commissioner pursuant to chapter 48.02 or 48.43 RCW;

(vii) The federal driver's privacy protection act of 1994, 18 U.S.C. Sec. 2721 et seq.;

(viii) The federal family educational rights and privacy act, 20 U.S.C. Sec. 1232g et seq.; or

(ix) The federal farm credit act of 1971, 12 U.S.C. Sec. 2001 et seq.;

(m) Personal data collected, processed, sold, or disclosed in relation to price, route, or service, as such terms are used in the airline deregulation act, 49 U.S.C. Sec. 40101 et seq., by an air carrier subject to the act, to the extent this chapter is preempted by the airline deregulation act, 49 U.S.C. Sec. 41713;

(n) Data processed or maintained:

(i) In the course of 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 the individual under this chapter 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 (n)(i) of this subsection and used for the purposes of administering such benefits;

(o) Personal data collected and processed solely for the journalistic purposes of gathering or reporting of news or information to the public by news media as defined in RCW 5.68.010,

if the controller reasonably believes that the collection and processing of such data is in the public interest and that the journalistic purpose served by the collection and processing is incompatible with this chapter; or

(p) Information collected by or disclosed to the national insurance crime bureau, the national association of insurance commissioners, or a similar organization under RCW 48.135.050.

(4) Controllers that are in compliance with the verifiable parental consent requirements under the children's online privacy protection act, 15 U.S.C. Secs. 6501 through 6506 and its implementing regulations, are deemed compliant with any obligation to obtain parental consent under this chapter.

NEW SECTION. **Sec. 3.** CONSUMER RIGHTS. (1) A consumer has the right to:

(a) Confirm whether a controller is collecting or processing personal data concerning the consumer, access such personal data, and confirm whether or not the consumer's personal data is used to profile the consumer for the purpose of automated decision making;

(b) Obtain from a controller a list of specific third parties, other than natural persons, to which the controller has transferred either the consumer's personal data or any personal data;

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

(d) Delete personal data concerning the consumer, including personal data the consumer provided to the controller, personal data the controller obtained from another source, and derived data;

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

(f) Opt out of the processing of the personal data for purposes of:

(i) Targeted advertising;

(ii) The sale of personal data; or

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

(2)(a) If a consumer's personal data is profiled in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer, the consumer has the right to question the result of such profiling, to be informed of the reason why the profiling resulted in the decision, and, if feasible, to be informed of what actions the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future.

(b) The consumer has the right to review the consumer's personal data used in the profiling.

(c) If the decision is determined to have been based upon inaccurate personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

NEW SECTION. **Sec. 4.** EXERCISING CONSUMER RIGHTS. (1) A consumer may exercise rights under this chapter by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice.

(2)(a) A consumer may designate another person to serve as the consumer's authorized agent, and act on the consumer's behalf, to exercise rights specified in section 3 of this act.

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

(3) In the case of personal data of a known child, the parent or legal guardian of the known child may exercise the rights of this chapter on the child's behalf.

(4) In the case of personal data concerning a consumer subject to guardianship, conservatorship, or other protective arrangement, the guardian or the conservator of the consumer may exercise the rights of this chapter on the consumer's behalf.

NEW SECTION. **Sec. 5.** RESPONDING TO CONSUMER REQUESTS. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized in this chapter in accordance with this section.

(1) A controller shall respond to the consumer without undue delay, but not later than 45 days after receipt of the request. The

response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.

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

(3) Information provided in response to a consumer request must be provided by the controller, free of charge, twice per consumer during any 12-month period. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

(4)(a) If a controller is unable to authenticate the request using commercially reasonable efforts, the controller is not required to comply with a request to exercise any of the rights under section 3 of this act and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(b) A controller may not require authentication of 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 such 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, stating that the controller believes the request to be fraudulent, why the controller believes the request to be fraudulent, and that the controller will not comply with the request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer is deemed in compliance with a consumer's request to delete such data pursuant to section 3(1)(d) of this act by deleting the consumer's personal data retained by the controller and 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 such retained data for any other purpose pursuant to this chapter.

(6) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process must be conspicuously available and similar to the process for submitting consumer rights requests. Within 45 days of 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.

(7) A controller may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a consumer right described in section 3 of this act through the use of dark patterns or any false, fictitious, fraudulent, or materially misleading statement or representation.

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

(9) A controller shall establish, and describe in the controller's privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this chapter. Such means must take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to verify the identity of the consumer making the request. Such means must include:

(a) Providing a clear and conspicuous link on the controller's internet website to an internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising, the sale of the consumer's personal data, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer; and

(b) Not later than December 31, 2025, allowing a consumer to opt out of any collection or processing of the consumer's personal data for the purposes of targeted advertising, or any sale of the consumer's personal data, through an opt-out preference signal that

is sent, with the consumer's consent, by a platform, technology, or mechanism to the controller and that indicates the consumer's intent to opt out of any processing or sale. The platform, technology, or mechanism must:

(i) Be consumer friendly and easy to use by the average consumer; and

(ii) Enable the controller to reasonably determine that the consumer is a Washington resident and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising. For purposes of this subsection, the use of an internet protocol address to estimate the consumer's location shall be considered sufficient to reasonably determine residency.

(10) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of the consumer's personal data, through an opt-out preference signal sent in accordance with subsection (9) of this section conflicts with the consumer's existing controller specific privacy setting or voluntary participation in a controller's financial incentive program, the controller shall comply with the consumer's opt-out preference signal, but may notify the consumer of the conflict and provide to the consumer the choice to confirm the controller specific privacy setting or participation in the program.

(11) If a controller responds to the consumer opt-out requests received pursuant to subsection (9) of this section by informing the consumer of a change in the price, rate, level, quality, or selection of goods or services, the controller shall present the terms of any financial incentive offered pursuant to section 6(7) of this act for the retention, use, sale, or sharing of the consumer's personal data.

NEW SECTION. **Sec. 6.** RESPONSIBILITIES OF CONTROLLERS. (1)(a) Except as specified in (b) of this subsection, a controller shall limit the collection, processing, and transfer of personal data to what is strictly necessary in relation to provide or maintain:

(i) A specific product or service requested by the consumer to whom the data pertains, including any routine administrative, operational, or account-servicing activity, such as billing, shipping, delivery, storage, or accounting; or

(ii) A communication, that is not an advertisement, by the controller to the consumer reasonably anticipated within the context of the relationship between the controller and the consumer.

(b) A controller may only collect and transfer consumer health data in accordance with RCW 19.373.030.

(c) Except with respect to sensitive data, a controller may process or transfer personal data collected under this subsection to provide first-party advertising or targeted advertising. However, this subsection does not permit the processing or transfer of personal data for targeted advertising to a consumer who has opted out of such advertising pursuant to this chapter or to a consumer under circumstances where the controller has knowledge, or willfully disregards, that the consumer is a minor.

(2) Except as specified in RCW 19.373.030, a controller may not transfer sensitive data concerning a consumer without obtaining the consumer's affirmative consent, or, in the case of the collection or processing of sensitive data of a known child, without collecting or processing such data in accordance with the children's online privacy protection act, 15 U.S.C. Sec. 6501 through 6506 and its implementing regulations.

(3) A controller may not sell sensitive data, with the exception of consumer health data, which may be sold in accordance with RCW 19.373.070.

(4) A controller shall establish, implement, and maintain administrative, technical, and physical data security practices that, at a minimum, satisfy reasonable standard of care within the controller's industry to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue, including disposing of personal data in accordance with a retention schedule that requires the deletion of personal data when the data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected, processed, or transferred.

(5) A controller shall provide an effective mechanism for a consumer to revoke the consumer's affirmative consent that is at least as easy as the mechanism by which the consumer provided the consumer's affirmative consent. Upon revocation of the consumer's affirmative consent, the controller shall cease to process the data as soon as practicable, but not later than 15 days after the receipt of the revocation.

(6) A controller may not process the personal data of a consumer for purposes of targeted advertising or sell the consumer's personal data under the circumstances where a controller has actual knowledge, or willfully disregards, that the consumer is a minor.

(7)(a) A controller may not discriminate or retaliate against a consumer for exercising any of the consumer rights contained in this chapter, or for refusing to agree to the collection or processing of personal data for a separate product or service, including by 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.

(b) Nothing in this subsection may be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain.

(c)(i) Nothing in this subsection may be construed to 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 offering is in connection with a consumer's voluntary participation in a financial incentive program, such as a bona fide loyalty, rewards, premium features, discounts, or club card program, provided that the controller may not transfer personal data to a third party as part of such a program unless:

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

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

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

(ii) The sale of personal data must not be considered functionally necessary to provide a financial incentive program. A controller may not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

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

(b) This subsection does not apply to:

(i) The collection, processing, or transfer of personal data for the sole purpose of a controller's or processor's self-testing to prevent or mitigate unlawful discrimination or otherwise to ensure compliance with state or federal law, or for the sole purpose of diversifying an applicant, participant, or customer pool; or

(ii) A private establishment, as described in 42 U.S.C. Sec. 2000a(e).

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

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

(ii) The categories of sources from which the consumer health data is collected;

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

(iv) How consumers may exercise their consumer rights included in section 3 of this act, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(v) The categories of personal data that the controller transfers to third parties, if any, and the purposes for those transfers;

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

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

(viii) An active email address or other online mechanism that the consumer may use to contact the controller.

(b) If a controller makes a material change to its privacy notice, the controller shall notify each consumer affected by the material change before implementing the material change with respect to prospectively collected personal data and provide a reasonable opportunity for each consumer to withdraw consent. A controller should provide a reasonable opportunity for each consumer to

affirmatively consent to further materially different processing or transfer of previously collected personal data under the changed policy. The controller shall take all reasonable electronic measures to provide direct notification regarding material changes to the privacy notice to each affected consumer, taking into account available technology and the nature of the relationship.

(10) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such selling or processing, as well as the manner in which a consumer may exercise the right to opt out of such selling or processing. The sale of consumer health data must comply with RCW 19.373.030.

NEW SECTION. **Sec. 7.** RESPONSIBILITIES OF PROCESSORS. (1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter. A processor's assistance must include:

(a) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, assisting the controller in fulfilling the controller's obligation to respond to consumer rights requests;

(b) Taking into account the nature of processing and the information available to the processor, assisting the controller in meeting the controller's obligation in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the processor's system in order to meet the controller's obligations; and

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

(2) The processor's data processing procedures with respect to processing performed on behalf of the controller must be governed by a contract between a controller and a processor. The contract must be binding and must clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The processor shall adhere to the instructions of the controller and only process and transfer data it receives from the controller to the extent necessary to provide a

service requested by the controller, as set out in the contract. The contract must also require that the processor:

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

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

(c) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with this chapter;

(d) After providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data;

(e) Be prohibited from combining personal data that the processor receives from or on behalf of a controller with personal data that the processor receives from or on behalf of another person or collects from the interaction of the processor with an individual; and

(f) Allow and cooperate with reasonable assessments by the controller or the controller's designated assessor or arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

(3) A processor shall establish, implement, and maintain administrative, technical, and physical data security practices that, at a minimum, satisfy reasonable standard of care within the processor's industry to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

(4) 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 this chapter.

(5) 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 who is not limited in the processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to that 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 such processing and may be subject to an enforcement action under this chapter.

NEW SECTION. **Sec. 8.** DATA PROTECTION ASSESSMENTS. (1) A controller may not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment for each of the controller's processing activities that presents the heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:

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

(b) The sale of personal data;

(c) The processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of:

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

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

(iii) A physical or other intrusion upon the solitude, seclusion, or the private affairs or concerns of consumers, where such intrusion would be offensive to a reasonable person; or

(iv) Other substantial injury to consumers; and

(d) The collection or processing of sensitive data.

(2) Data protection assessments conducted pursuant to subsection (1) of this section must identify the categories of personal data collected, the purposes for collecting personal data, and whether personal data is being transferred. Data protection assessments must also identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the

rights of the consumer associated with such processing, as mitigated by safeguards that are employed by the controller to reduce such risks. The controller shall factor into any data protection assessment the use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data is being processed.

(3)(a) A controller shall submit a report of the data protection assessment or evaluation to the attorney general upon request. The report must include a summary of the data protection assessment, and the controller shall make the summary publicly available in a place that is easily accessible to consumers.

(b) The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller shall make the data protection assessment available to the attorney general upon request. The attorney general may evaluate the data protection assessment for compliance with the responsibilities set forth in this chapter. To the extent any information contained in a data protection assessment disclosed to the attorney general includes information subject to attorney-client privilege or work product protection, the disclosure does not constitute a waiver of such privilege or protection.

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

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

(6) A controller shall conduct and document a data protection assessment before initiating a processing activity that presents a heightened risk of harm to a consumer. Throughout the processing activity's life cycle, the controller shall review and update the data protection assessment as often as appropriate, taking into consideration the type, amount, and sensitivity of personal data collected or processed and the level of risk presented by the processing, in order to:

(a) Monitor for harm caused by the processing and adjust safeguards accordingly; and

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

(7) The first data protection assessment required by this section must be completed no later than one year after the effective date of this section.

NEW SECTION. **Sec. 9.** DEIDENTIFIED DATA. (1) Any controller in possession of deidentified data shall:

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

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

(c) Contractually obligate any recipients of the deidentified data to comply with all provisions of this chapter.

(2) Nothing in this chapter may be construed to require a controller or processor to:

(a) Reidentify deidentified data;

(b) Maintain data in an identifiable form; or

(c) Collect, obtain, retain, or access any data or technology in order to be capable of associating an authenticated consumer request with personal data.

(3) Nothing in this chapter may be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

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

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

(4) A controller that transfers 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 those contractual commitments.

NEW SECTION. **Sec. 10.** LIMITATIONS. (1) The obligations imposed on controllers and processors under this chapter do not restrict a controller's or processor's ability to:

(a) Comply with federal, state, or local laws, rules, or regulations, except as prohibited by the Washington shield law, chapter 7.115 RCW;

(b) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental 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 local laws, rules, or regulations;

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

(e) Provide a product or service specifically requested by the 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 into 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 where 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 targeted at or involving the controller or processor or its services; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

(j) Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all relevant laws and regulations governing such research, if applicable, and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that determines whether:

(i) The deletion of personal data requested by a consumer pursuant to section 3 of this act is likely to provide substantial benefits that do not exclusively accrue to the controller;

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

(iii) The controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification;

(k) Assist another controller, processor, or third party with any of the obligations under this chapter;

(l) Process personal data for reasons of public interest in the area of public health, community health, or population health, but solely to the extent that such processing is:

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

(ii) Under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law;

(m) Ensure the data security and integrity of personal data as required by this chapter, protect against spam, or protect and maintain networks and systems, including through diagnostics, debugging, and repairs;

(n) Transfer assets to a third party in the context of a merger, acquisition, bankruptcy, or similar transaction when the third party assumes control, in whole or in part, of the controller's assets, provided that the controller, in a reasonable time prior to the transfer, provides an affected consumer with notice describing the transfer, including the name of the entity receiving the consumer's personal data and the applicable privacy policies of such entity, and a reasonable opportunity to withdraw previously provided consent related to the consumer's personal data and to request the deletion of the consumer's personal data;

(o) Effectuate a product recall pursuant to federal or state law, or to fulfill a warranty;

(p) Conduct medical research in compliance with 45 C.F.R. Part 46 or 21 C.F.R. Part 50 or 56; or

(q) Process personal data previously collected in accordance with this chapter such that the personal data becomes deidentified data, including to:

(i) Conduct internal research to develop, improve, or repair products, services, or technology;

(ii) Identify and repair technical errors that impair existing or intended functionality; or

(iii) 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.

(2) The obligations imposed on controllers and processors under this chapter do not apply where compliance by a controller or processor would violate an evidentiary privilege under Washington law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Washington law as part of a privileged communication.

(3) A controller or processor that discloses personal data in compliance with this chapter to a third-party controller or processor is not in violation of this chapter if the recipient processes such personal data in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient would violate this chapter. A third-party controller or processor receiving personal data in compliance with this chapter from a controller or processor is likewise not in violation of this chapter for the transgressions of the controller or processor from which it receives the personal data.

(4) Nothing in this chapter may be construed to:

(a) Impose any obligation on a controller or processor that adversely affects the rights or freedoms of any persons including, but not limited to, the rights of any person to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution or under the Washington reporter shield law, chapter 5.68 RCW;

(b) Apply to any person's collection or processing of personal data in the course of the person's purely personal or household activities; or

(c) For private schools approved by the state under chapter 28A.195 RCW and private institutions of higher education as defined in 20 U.S.C. Sec. 1001 et seq., require deletion of personal data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution.

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

(i) Strictly necessary and proportionate to the purposes listed in this section, or, in the case of consumer health data, is in compliance with RCW 19.373.030;

(ii) Limited to what is strictly necessary in relation to the specific purpose or purposes listed in this section, or, in the case of consumer health data, in compliance with RCW 19.373.030; and

(iii) Compliant with section 6 of this act.

(b) Personal data processed pursuant to subsection (1)(q) of this section must, where applicable, take into account the nature and purpose or purposes of the processing. Such 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 such processing of personal data.

(6) If a controller collects or processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such collection or processing qualifies for the exemption and complies with the requirements in subsection (5) of this section.

NEW SECTION. **Sec. 11.** ADDITIONAL REQUIREMENTS. (1) Controllers and processors that collect or process consumer health data may be subject to additional data privacy requirements pursuant to chapter 19.373 RCW.

(2) Controllers and processors that collect or process data that is exempt from this chapter may still be considered regulated entities or processors under chapter 19.373 RCW and may be required to comply with obligations under chapter 19.373 RCW.

NEW SECTION. **Sec. 12.** ENFORCEMENT. The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW.

NEW SECTION. **Sec. 13.** RIGHT TO CURE. (1) Before bringing an action under section 12 of this act, the attorney general shall notify a controller or processor of the alleged violation if the attorney general determines that a cure is possible. If the controller or processor fails to cure the violation within 30 days after receiving notice of the violation, the attorney general may bring a civil action without further notice.

(2) This section expires August 1, 2027.

NEW SECTION. **Sec. 14.** OTHER ENFORCEMENT PRECLUDED. The rights and obligations created by this chapter may only be enforced pursuant to sections 12 and 13 of this act.

NEW SECTION. **Sec. 15.** WAIVER OF RIGHTS. Any provision of a contract or agreement of any kind that purports to waive, release, limit in any way, or extinguish the rights of consumers under this chapter is against public policy and is void and unenforceable.

NEW SECTION. **Sec. 16.** A new section is added to chapter 19.373 RCW to read as follows:

A regulated entity, small business, or processor subject to the requirements of this chapter may also be subject to data privacy requirements provided in chapter 19.--- RCW (the new chapter created in section 18 of this act).

NEW SECTION. **Sec. 17.** If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

NEW SECTION. **Sec. 18.** Sections 1 through 12 and 14 and 15 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. **Sec. 19.** Sections 12 and 13 of this act take effect August 1, 2026.

--- END ---