SUBSTITUTE HOUSE BILL 1850

State of Washington 67th Legislature 2022 Regular Session

By House Civil Rights & Judiciary (originally sponsored by Representatives Slatter, Berg, Pollet, and Harris-Talley)

READ FIRST TIME 02/03/22.

AN ACT Relating to protecting and enforcing the foundational data privacy rights of Washingtonians; adding a new section to chapter 42.56 RCW; adding a new chapter to Title 19 RCW; creating new sections; prescribing penalties; and providing effective dates.

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

NEW SECTION. **Sec. 1.** SHORT TITLE. This act may be known and cited as the Washington foundational data privacy act.

NEW SECTION. **Sec. 2.** LEGISLATIVE FINDINGS AND INTENT. (1) The legislature finds that the people of Washington regard their privacy as a fundamental right and an essential element of their individual freedom. Washington's Constitution explicitly provides the right to privacy, and fundamental privacy rights have long been and continue to be integral to protecting Washingtonians and to safeguarding our democratic republic.

(2) Ongoing advances in technology have produced an exponential growth in the volume and variety of personal data being generated, collected, stored, and analyzed, which presents both promise and potential peril. The ability to harness and use data in positive ways is driving innovation and brings beneficial technologies to society. However, it has also created risks to privacy and freedom. The

unregulated and unauthorized use and disclosure of personal information and loss of privacy can have devastating impacts, ranging from financial fraud, identity theft, and unnecessary costs, to personal time and finances, to destruction of property, harassment, reputational damage, emotional distress, and physical harm.

(3) Given that technological innovation and new uses of data can help solve societal problems, protect public health associated with global pandemics, and improve quality of life, the legislature seeks to shape responsible public policies where innovation and protection of individual privacy coexist. The legislature notes that our federal authorities have not developed or adopted into law regulatory or legislative solutions that give consumers control over their privacy. In contrast, the European Union's general data protection regulation has continued to influence data privacy policies and practices of those businesses competing in global markets. In the absence of federal standards, Washington will join a growing number of states across the country to empower consumers to protect their privacy and require companies to be responsible custodians of data as they continue to innovate.

(4) With this act, the legislature intends to: Provide a modern privacy regulatory framework with data privacy guardrails to protect individual privacy; establish mechanisms for consumers to exercise control over their data; and require companies to be responsible custodians of data as technological innovations emerge.

(5) This act gives consumers the ability to protect their own rights to privacy by explicitly providing consumers the right to access, correct, and delete personal data, as well as the rights to obtain data in a portable format and to opt out of or into the collection and use of personal data for certain purposes. These rights will add to, and not subtract from, the consumer protection rights that consumers already have under Washington state law.

(6) This act also imposes affirmative obligations upon companies to safeguard personal data, and provide clear, understandable, and transparent information to consumers about how their personal data is used. It strengthens compliance and accountability by requiring data protection assessments in the collection and use of personal data. It empowers the state attorney general to obtain and evaluate a company's data protection assessments, to conduct investigations, while preserving consumers' rights under the consumer protection act to impose penalties where violations occur, and to prevent against

future violations. Finally, it creates a new privacy commission to regulate how businesses process and control consumer data.

NEW SECTION. **Sec. 3.** DEFINITIONS. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with, that other legal entity. For these purposes, "control" or "controlled" means: Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company; control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company.

(2) "Air carriers" has the same meaning as defined in the federal aviation act (49 U.S.C. Sec. 40101, et seq.), including the airline deregulation act (49 U.S.C. 41713).

(3) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights in section 5 (1) through (4) of this act is being made by the consumer who is entitled to exercise such rights with respect to the personal data at issue.

(4) "Business associate" has the same meaning as in Title 45 C.F.R., established pursuant to the federal health insurance portability and accountability act of 1996.

(5) "Child" has the same meaning as defined in the children's online privacy protection act, Title 15 U.S.C. Sec. 6501 through 6506.

(6) "Commission" means the Washington state consumer data privacy commission created in section 14 of this act.

(7) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer signifies agreement to the processing of personal data relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through dark patterns does not constitute consent.

(8) "Consumer" means a natural person who is a Washington resident acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

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

(10) "Covered entity" has the same meaning as defined in Title 45 C.F.R., established pursuant to the federal health insurance portability and accountability act of 1996.

(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 effects concerning a consumer or similarly significant effects concerning a consumer" means decisions that result in the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

(13) "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to such a person, provided that the controller that possesses the data: (a) Takes reasonable measures to ensure that the data cannot be associated with a natural person, household, or device; (b) publicly commits to maintain and use the data only in a deidentified fashion and not attempt to reidentify the data; and (c) contractually obligates any recipients of the information to comply with all provisions of this subsection.

(14) "Device" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.

(15) "Health care facility" has the same meaning as defined in RCW 70.02.010.

(16) "Health care information" has the same meaning as defined in RCW 70.02.010.

(17) "Health care provider" has the same meaning as defined in RCW 70.02.010.

(18) "Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly.

(19) "Institutions of higher education" has the same meaning as in RCW 28B.92.030.

(20) "Judicial branch" means any court, agency, commission, or department provided in Title 2 RCW.

(21) "Known child" means a child under circumstances where a controller has actual knowledge of, or willfully disregards, the child's age.

(22) "Legislative agencies" has the same meaning as defined in RCW 44.80.020.

(23) "Local government" has the same meaning as in RCW 39.46.020.

(24) "Minor" means an individual who is at least 13 and under 16 years of age under circumstances where a controller has actual knowledge of, or willfully disregards, the minor's age.

(25) "Nonprofit corporation" has the same meaning as in RCW 24.03.005.

(26) "Personal data" means any information, including pseudonymous data, that is linked or reasonably linkable to an identified or identifiable natural person, household, or consumer device. "Personal data" does not include deidentified data or publicly available information.

(27) "Process" or "processing" means any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(28) "Processor" means a natural or legal person who processes personal data on behalf of a controller.

(29) "Profiling" means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(30) "Protected health information" has the same meaning as defined in Title 45 C.F.R., established pursuant to the federal health insurance portability and accountability act of 1996.

(31) "Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational

measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

(32) "Publicly available information" means information that is lawfully made available from federal, state, or local government records.

(33) "Share," "shared," or "sharing" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal data by the controller to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.

(34) "Sensitive data" means (a) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sexual orientation, or citizenship or immigration status; (b) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; (c) the personal data from a known child; or (d) specific geolocation data. "Sensitive data" is a form of personal data.

(35) "Specific geolocation data" means information derived from technology including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms that directly identifies the specific location of a natural person within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet. Specific geolocation data excludes the content of communications.

(36)(a) "Targeted advertising" means obtaining information about a consumer to direct or display an advertisement to the consumer that is selected based in whole or in part on personal data about the consumer.

(b) "Targeted advertising" does not include displaying advertisements to a consumer based solely upon the consumer's current visit to a website, application, service, or controller, or in direct response to the consumer's request for information or feedback.

(37) "Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller.

NEW SECTION. **Sec. 4.** JURISDICTIONAL SCOPE. (1) This chapter applies to legal entities that conduct business in Washington or produce products or services that are targeted to residents of Washington, and that satisfy one or more of the following thresholds:

(a) During a calendar year, control or process personal data of 100,000 consumers or more; or

(b) Derive over 25 percent of gross revenue from the sharing of personal data and control or process personal data of 25,000 consumers or more.

(2) This chapter does not apply to:

(a) State agencies, legislative agencies, the judicial branch, local governments, or tribes;

(b) Municipal corporations;

(c) Air carriers;

(d) Nonprofit organizations that:

(i) Are registered with the secretary of state under the charities program pursuant to chapter 19.09 RCW;

(ii) Collect personal data during legitimate activities related to the organization's tax-exempt purpose; and

(iii) Do not share personal data collected by the organization;

(e) The national insurance crime bureau, the national association of insurance commissioners, or a similar organization to which any insurer or licensee of the state insurance commissioner must disclose information related to insurance fraud pursuant to RCW 48.135.050;

(f) Information that meets the definition of:

(i) Protected health information for purposes of the federal health insurance portability and accountability act of 1996 and related regulations;

(ii) Health care information for purposes of chapter 70.02 RCW;

(iii) Patient identifying information for purposes of 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

(iv) Identifiable private information for purposes of the federal policy for the protection of human subjects, 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; the protection of human subjects under 21 C.F.R. Parts 50 and 56; or personal data used or shared in research conducted in accordance with one or more of the requirements set forth in this subsection;

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

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

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

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

(D) 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);

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

(vii) Patient safety work product for purposes of 42 C.F.R. Part 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26; or

(viii) Information that is (A) deidentified in accordance with the requirements for deidentification set forth in 45 C.F.R. Part 164, and (B) derived from any of the health care-related information listed in this subsection (2)(f);

(g) Information originating from, and intermingled to be indistinguishable with, information under (f) 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;

(h) Information used only for public health activities and purposes as described in 45 C.F.R. Sec. 164.512;

(i)(i) An activity involving the collection, maintenance, disclosure, sharing, communication, or use of any personal data bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in Title 15 U.S.C. Sec. 1681a(f), by a furnisher of information, as set forth in Title 15 U.S.C. Sec. 1681s-2, who provides information for use in a consumer report, as defined in Title 15 U.S.C. Sec. 1681a(d), and by a user of a consumer report, as set forth in Title 15 U.S.C. Sec. 1681b.

(ii) (i)(i) of this subsection applies only to the extent that such an activity involving the collection, maintenance, disclosure, sharing, communication, or use of such personal data by that agency, furnisher, or user is subject to regulation under the fair credit reporting act, Title 15 U.S.C. Sec. 1681 et seq., and the personal data is not collected, maintained, used, communicated, disclosed, or shared except as authorized by the fair credit reporting act;

(j) Personal data collected and maintained for purposes of chapter 43.71 RCW;

(k) Personal data collected, processed, shared, or disclosed pursuant to the federal Gramm-Leach-Bliley act (P.L. 106-102), and implementing regulations, if the collection, processing, sharing, or disclosure is in compliance with that law;

(l) Personal data collected, processed, shared, or disclosed pursuant to the federal driver's privacy protection act of 1994 (18 U.S.C. Sec. 2721 et seq.), if the collection, processing, sharing, or disclosure is in compliance with that law;

(m) Personal data regulated by the federal family education rights and privacy act, 20 U.S.C. Sec. 1232g and its implementing regulations;

(n) Personal data regulated by the student user privacy in education rights act, chapter 28A.604 RCW;

(o) Personal data collected, maintained, disclosed, or otherwise used in connection with the gathering, dissemination, or reporting of news or information to the public by news media as defined in RCW 5.68.010(5);

(p) Personal data collected, processed, shared, or disclosed pursuant to the federal farm credit act of 1971 (as amended in 12 U.S.C. Sec. 2001-2279cc) and its implementing regulations (12 C.F.R. Part 600 et seq.) if the collection, processing, sharing, or disclosure is in compliance with that law; or

(q) Data collected or maintained: (i) In the course of an individual acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that it is collected and used solely within the context of that role; (ii) as the emergency contact information of an individual under (q)(i) of this subsection used solely for emergency contact purposes; or (iii) that is necessary for the business to retain to administer benefits for another individual relating to the individual under (q)(i) of this subsection is used solely for the purposes of administering those benefits.

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

(4) Payment-only credit, check, or cash transactions where no data about consumers are retained do not count as "consumers" for purposes of subsection (1) of this section.

NEW SECTION. **Sec. 5.** CONSUMER RIGHTS. (1) A consumer has the right to confirm whether or not a controller is processing personal data concerning the consumer and access the personal data the controller is processing.

(2) A consumer has the right to correct inaccurate personal data concerning the consumer.

(3) A consumer has the right to delete personal data concerning the consumer, including data from all parts of a controller or processor's network and backup systems.

(4) A consumer has the right to obtain personal data concerning the consumer, which the consumer previously provided to the controller, in a portable and, to the extent technically feasible, readily usable format that allows the individual to transmit the data to another controller without hindrance, where the processing is carried out by automated means.

(5) A consumer has the right to opt out of the processing of personal data concerning such a consumer for the purposes of (a) targeted advertising; (b) the sharing of personal data; or (c) profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer.

NEW SECTION. **Sec. 6.** EXERCISING CONSUMER RIGHTS. (1) A consumer or a consumer's authorized agent may exercise the rights set forth in section 5 of this act by submitting a request, at any time, to a controller specifying which rights the consumer wishes to exercise.

(2) A consumer may exercise the rights under section 5(5) (a) and (b) of this act:

(a) By designating an authorized agent who may exercise the rights on behalf of the consumer; or

(b) Via user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicates or signals the consumer's choice to opt out.

(3) In the case of processing 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 processing personal data concerning a consumer subject to guardianship, conservatorship, or other protective arrangement under chapter 11.88, 11.92, or 11.130 RCW, the guardian or the conservator of the consumer may exercise the rights of this chapter on the consumer's behalf.

NEW SECTION. **Sec. 7.** RESPONDING TO REQUESTS. (1) Except as provided in this chapter, the controller must comply with a request to exercise the rights pursuant to section 5 of this act.

(2)(a) Controllers must provide one or more secure and reliable means for consumers and a consumer's authorized agent to submit a request to exercise their rights under this chapter. These means must take into account the ways in which consumers interact with the controller and the need for secure and reliable communication of the requests.

(b) Controllers may not require a consumer to create a new account in order to exercise a right, but a controller may require a consumer to use an existing account to exercise the consumer's rights under this chapter.

(3) A controller must comply with a request to exercise the right in section 5(5) of this act as soon as feasibly possible, but no later than 15 days of receipt of the request.

(4)(a) A controller must inform a consumer of any action taken on a request to exercise any of the rights in section 5 (1) through (4) of this act without undue delay and in any event within 45 days of receipt of the request. That period may be extended once by 45 additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(b) If a controller does not take action on the request of a consumer, the controller must inform the consumer without undue delay and at the latest within 45 days of receipt of the request of the reasons for not taking action and instructions for how to appeal the decision with the controller as described in subsection (5) of this section.

(c) Information provided under this section must be provided by the controller to the consumer free of charge, up to twice annually. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (i) Charge a reasonable fee to cover the administrative costs of complying with the request; or (ii) refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(d) A controller is not required to comply with a request to exercise any of the rights under section 5 (1) through (4) of this act if the controller is unable to authenticate the request using commercially reasonable efforts. In such a case, the controller may request the provision of additional information reasonably necessary to authenticate the request.

(5)(a) A controller must establish an internal process whereby a consumer may appeal a refusal to take action on a request to exercise any of the rights under section 5 of this act within a reasonable period of time after the controller refuses to take action on such request.

(b) The appeal process must be conspicuously available and as easy to use as the process for submitting such a request under this section.

(c) Within 30 days of receipt of an appeal, a controller must inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support thereof. That period may be extended by 60 additional days where reasonably necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The controller must inform the consumer of such an extension within 30 days of receipt of the appeal, together with the reasons for the delay. The controller must also provide the consumer with an email address or other online mechanism through which the consumer may submit the appeal, along with any action taken or not taken by the controller in response to the appeal and the controller's written explanation of the reasons in support thereof, to the attorney general.

(d) When informing a consumer of any action taken or not taken in response to an appeal pursuant to (c) of this subsection, the controller must clearly and prominently provide the consumer with information about how to file a complaint with the commission. The controller must maintain records of all such appeals and how it responded to them for at least 24 months and shall, upon request, compile and provide a copy of such records to the attorney general.

NEW SECTION. **Sec. 8.** RESPONSIBILITY ACCORDING TO ROLE. (1) Controllers and processors are responsible for meeting their respective obligations established under this chapter.

(2) Processors are responsible under this chapter for adhering to the instructions of the controller and assisting the controller to meet its obligations under this chapter. This assistance includes the following:

(a) Taking into account the nature of the processing, the processor shall assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to section 5 of this act; and

(b) Taking into account the nature of processing and the information available to the processor, the processor shall: Assist the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system pursuant to RCW 19.255.010; and provide information to the controller necessary to enable the controller to conduct and document any data protection assessments required by section 11 of this act. The controller and processor are each responsible for only the measures allocated to them.

(3) Notwithstanding the instructions of the controller, a processor shall:

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

(b) Engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract in accordance with subsection (5) of this section that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(4) Taking into account the context of processing, the controller and the processor shall implement appropriate technical and

organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement such measures.

(5) Processing by a processor must be governed by a contract between the controller and the processor that is binding on both parties and that sets out the processing instructions to which the processor is bound, including the nature and purpose of the processing, the type of personal data subject to the processing, the duration of the processing, and the obligations and rights of both parties. In addition, the contract must include the requirements imposed by this subsection and subsections (3) and (4) of this section, as well as the following requirements:

(a) At the choice of the controller, the processor shall 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;

(b)(i) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this chapter; and

(ii) The processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. Alternatively, the processor may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, an audit 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 audit procedure for the audits as applicable, and provide a report of the audit to the controller upon request.

(6) In no event may any contract relieve a controller or a processor from the liabilities imposed on them by virtue of its role in the processing relationship as defined by this chapter.

(7) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed. A person that is not limited in its processing of personal data pursuant to a controller's instructions, or that fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of 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, it is a controller with respect to the processing.

NEW SECTION. **Sec. 9.** RESPONSIBILITIES OF CONTROLLERS. (1)(a) Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(i) The categories of personal data processed by the controller;

(ii) The purposes for which the categories of personal data are processed;

(iii) How and where consumers may exercise the rights contained in section 5 of this act, including how a consumer may appeal a controller's action with regard to the consumer's request;

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

(v) The categories of third parties, if any, with whom the controller shares personal data.

(b) If a controller shares personal data with third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose the processing, as well as the manner in which a consumer may exercise the right to opt out of the processing, in a clear and conspicuous manner.

(c) The privacy notice required under this subsection must:

(i) Use clear and plain language;

(ii) Be in English and any other language in which a controller communicates with the consumer to whom the information pertains; and

(iii) Be understandable to the least sophisticated consumer.

(2) A controller's collection, use, sharing, and retention of personal data must be limited to what is reasonably necessary in relation to the purposes for which the data is processed.

(3) A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the purposes for which the data is processed.

(4) Except as provided in this chapter, a controller may not process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which the personal data is processed unless the controller obtains the consumer's consent.

(5) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security

practices to protect the confidentiality, integrity, and accessibility of personal data. The data security practices must be appropriate to the volume and nature of the personal data at issue.

(6) A controller shall not process personal data on the basis of a consumer's or a class of consumers' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, lawful source of income, or disability, in a manner that unlawfully discriminates against the consumer or class of consumers with respect to the offering or provision of: (a) Housing; (b) employment; (c) credit; (d) education; or (e) the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation.

(7) A controller may not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. This subsection does not 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 bona fide loyalty, rewards, premium features, discounts, or club card program. If a consumer exercises their right pursuant to section 5(5) of this act, a controller may not share personal data with a third-party controller as part of such a program unless: (a) The sharing is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled; (b) the sharing of personal data to third parties is clearly disclosed in the terms of the program; and (c) the third party uses the personal data only for purposes of facilitating such a benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.

(8)(a) Except as otherwise provided in this chapter, a controller may not process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of the processing of sensitive data of a known child, without obtaining consent from the child's parent or lawful guardian, in accordance with the children's online privacy protection act requirements.

(b) A controller shall provide an effective mechanism for a consumer to revoke consent after it is given. After a consumer revokes consent, the controller shall cease processing the consumer's sensitive data as soon as practicable, but in no case any later than 15 days after the consumer's revocation of consent.

(9) Except as otherwise provided in this chapter, a controller may not process the personal data of a minor for the purposes of targeted advertising or the sharing of personal data without obtaining consent from the minor.

(10) Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this chapter is deemed contrary to public policy and is void and unenforceable.

NEW SECTION. **Sec. 10.** PROCESSING DEIDENTIFIED DATA OR PSEUDONYMOUS DATA. (1) This chapter does not require a controller or processor to do any of the following solely for purposes of complying with this chapter:

(a) Reidentify deidentified data;

(b) Comply with an authenticated consumer request to access, correct, delete, or port personal data pursuant to section 5 (1) through (4) of this act, if all of the following are true:

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

(ii) The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and

(iii) The controller does not share personal data with any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section; or

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

(2) The rights contained in section 5 (1) through (4) of this act do not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and

organizational controls that prevent the controller from accessing such information.

(3) A controller that uses pseudonymous data or deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data are subject and must take appropriate steps to address any breaches of contractual commitments.

NEW SECTION. **Sec. 11.** DATA PROTECTION ASSESSMENTS. (1) Controllers must conduct and document a data protection assessment of each of the following processing activities involving personal data:

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

(b) The processing of personal data for the purposes of the sharing of personal data;

(c) The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of: (i) Unfair or deceptive treatment of, or disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or 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;

(d) The processing of sensitive data; and

(e) Any processing activities involving personal data that present a heightened risk of harm to consumers.

Such data protection assessments must take into account the type of personal data to be processed by the controller, including the extent to which the personal data are sensitive data, and the context in which the personal data are to be processed.

(2) Data protection assessments conducted under subsection (1) of this section must identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, 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 can be employed by the controller to reduce such risks. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose

personal data will be processed, must be factored into this assessment by the controller.

(3) The attorney general may request, in writing, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. The controller must make a data protection assessment available to the attorney general upon such a request. The attorney general may evaluate the data protection assessments for compliance with the responsibilities contained in section 9 of this act and, if it serves a civil investigative demand, with RCW 19.86.110. Data protection assessments are confidential and exempt from public inspection and copying under chapter 42.56 RCW. The disclosure of a data protection assessment pursuant to a request from the attorney general under this subsection does not constitute a waiver of the attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment unless otherwise subject to case law regarding the applicability of attorney-client privilege or work product protections.

(4) Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may qualify under this section if they have a similar scope and effect.

NEW SECTION. **Sec. 12.** LIMITATIONS AND APPLICABILITY. (1) The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to do any of the following, to the extent that the processing of a consumer's personal data is reasonably necessary and proportionate for these purposes:

(a) Comply with federal, state, or local laws, rules, or regulations;

(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 a consumer, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;

(f) Take immediate steps to protect an interest that is essential for the life of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

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

(h) 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: (i) If the research 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) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

(i) Assist another controller, processor, or third party with any of the obligations under this subsection.

(2) The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to collect, use, or retain data to:

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

(b) Perform solely internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with processing 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 when those internal operations are performed during, and not following, the consumer's relationship with the controller.

(3) The obligations imposed on controllers or processors under this chapter do not apply where compliance by the controller or

processor with this chapter 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.

(4) A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this chapter 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 intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter is likewise not in violation of this chapter for the obligations of the controller or processor from which it receives such personal data.

(5) Obligations imposed on controllers and processors under this chapter shall not:

(a) Adversely affect the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution; or

(b) Apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

(6) Processing personal data solely for the purposes expressly identified in subsection (1)(a) through (g) of this section does not, by itself, make an entity a controller with respect to the processing.

(7) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements in subsection (8) of this section.

(8)(a) Personal data that is processed by a controller pursuant to this section must not be processed for any purpose other than those expressly listed in this section.

(b) Personal data that is processed by a controller pursuant to this section may be processed solely to the extent that such processing is: (i) Necessary, reasonable, and proportionate to the purposes listed in this section; (ii) adequate, relevant, and limited to what is necessary in relation to the specific purpose or purposes listed in this section; and (iii) insofar as possible, taking into account the nature and purpose of processing the personal data, subjected 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.

NEW SECTION. **Sec. 13.** ANNUAL REGISTRATION REQUIREMENT. (1) Annually, on or before January 31st following a year in which a controller or processor meets the jurisdictional scope thresholds as provided in section 4 of this act and is subject to the requirements of this chapter, the controller or processor shall:

(a) Register with the commission through a digital application developed and maintained by the commission;

(b) Provide the following information to the commission:

(i) The name and primary physical, email, and internet addresses of the controller or processor;

(ii) Whether the controller or processor offers an opt-in or opt-out model for its personal data processing operations and the specific details of how a consumer can access these options;

(iii) A statement specifying the methods used for personal data processing operations and databases maintained;

(iv) A statement specifying the number of data subject globally about whom personal data was collected, processed, or shared in the preceding year;

(v) A statement specifying the number of Washington consumers about whom personal data was collected, processed, or shared in the preceding year; and

(vi) Annual gross revenues of the controller or processor; and

(c) Pay a registration fee equal to:

(i) $250, if the controller or processor's annual gross revenue in the year preceding the registration is $850,000,000 or less; or

(ii) $450, if the controller or processor's annual gross revenue in the year preceding the registration is greater than $850,000,000.

(2) A controller or processor that fails to register as required by subsection (1)(a) of this section is subject to a fine between $1,000 and $20,000 for each day it fails to register pursuant to this section.

(3) A controller or processor that knowingly submits false or incomplete information required in subsection (1)(b) of this section is subject to a fine between $10,000 and $100,000.

(4) The fines under subsections (2) and (3) of this section must be levied by the commission. When determining the amount of fines to be levied, the commission shall consider factors such as the controller or processor's gross annual revenue and assets and whether the controller or processor made reasonable efforts to comply with the requirements of this section.

(5) All receipts from the registration fees and the imposition of fines under this section must be deposited into the consumer privacy account created in section 21 of this act.

NEW SECTION. **Sec. 14.** WASHINGTON STATE CONSUMER DATA PRIVACY COMMISSION. (1)(a) The Washington state consumer data privacy commission is created and is vested with full administrative power, authority, and jurisdiction to implement and enforce this chapter and the rules adopted under it by the commission.

(b) The commission is composed of three members to be appointed by the governor with the advice and consent of the senate, one of whom must be designated as chairperson by the governor.

(c) The term of each commissioner is five years. A commission member is eligible for reappointment.

(d) The commission may employ staff as necessary to carry out the commission's duties as prescribed in this chapter. The Washington utilities and transportation commission shall provide all administrative staff support for the commission, which shall otherwise retain its independence in exercising its powers, functions, and duties and its supervisory control over nonadministrative staff.

(e) The commission may appoint an executive director and set, within the limitations provided by law, the executive director's compensation. The executive director shall perform those duties and have those powers as the commission may prescribe and delegate to implement and enforce this chapter efficiently and effectively. The commission may not delegate its authority to:

(i) Adopt, amend, or rescind rules;

(ii) Determine that a violation of this chapter has occurred; or

(iii) Assess penalties for violations.

(2) Members of the commission shall:

(a) Have qualifications, experience, and skills, in particular in the areas of privacy and technology, required to perform the duties of the commission and exercise its powers and authority;

(b) Maintain the confidentiality of information that has come to their knowledge in the course of the performance of their tasks or exercise of their powers, except to the extent that disclosure is required by chapter 42.56 RCW;

(c) Remain free from external influence, whether direct or indirect, and neither seek nor take instructions from another;

(d) Refrain from any action incompatible with their duties or engage in any incompatible occupation, whether gainful or not, during their term;

(e) Have the right of access to all information made available by the commission to the chair of the commission;

(f) Be precluded, for a period of one year after leaving office, from accepting employment with a controller or processor that was subject to an enforcement action or civil action under this chapter during the member's tenure or during the five-year period preceding the member's appointment; and

(g) Be precluded for a period of two years after leaving office from acting, for compensation, as an agent or attorney for, or otherwise representing, any other person in a matter pending before the commission if the purpose is to influence an action of the commission.

NEW SECTION. **Sec. 15.** RULE-MAKING AUTHORITY OF THE WASHINGTON STATE CONSUMER DATA PRIVACY COMMISSION. The commission shall adopt, amend, and rescind suitable rules under the administrative procedure act, chapter 34.05 RCW, to carry out the purposes and provisions of this chapter including, but not limited to, adopting rules in the following areas:

(1) Amending and updating as needed the definitions in this chapter to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns;

(2) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that controllers are required to provide pursuant to this chapter are provided in a manner that may easily be understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer;

(3) Establishing rules and procedures for the following:

(a) To facilitate and govern the submission of requests by consumers, with the goal of minimizing the administrative burden on consumers and ensuring that consumers have the ability to exercise their choices without undue burden, while taking into account available technology, security concerns, and the burden on controllers;

(b) To govern a controller's determination to authenticate a consumer request, including standards for a controller's determination that a request cannot be authenticated using commercially reasonable efforts;

(c) To govern controllers' compliance with consumers' requests and to prevent controllers from engaging in deceptive or harassing conduct, including in retaliation against consumers for exercising their rights, while allowing controllers to inform consumers of the consequences of exercising consumer data rights;

(d) To govern the processing of personal data for an exempt purpose pursuant to section 12 of this act and to ensure that controllers and processors do not use any exemptions for the purpose of evading consumers' rights with regard to personal data;

(e) To define the nature and scope of the data processing purposes and activities that are reasonably necessary to, or compatible with, the purposes for which personal data is processed, as specified in the privacy notice pursuant to section 9 of this act, with the goal of ensuring that controllers obtain consumer consent where required by section 9(4) of this act; and

(f) To define the requirements and technical specifications for global privacy controls that consumers may use to exercise the right to opt out;

(4) Establishing any exceptions necessary to comply with state or federal law including, but not limited to, those relating to trade secrets and intellectual property rights, with the intention that trade secrets should not be disclosed in response to an authenticated consumer request; and

(5) Adopting additional rules as necessary to further the purposes of this chapter, with the goal of strengthening consumer privacy and incorporating public input while considering the legitimate operational interests of controllers and processors.

NEW SECTION. **Sec. 16.** DUTIES OF THE WASHINGTON STATE CONSUMER DATA PRIVACY COMMISSION. The commission shall perform the following functions:

(1) Administer, implement, and enforce through administrative actions this chapter and any rules or regulations adopted by the commission pursuant to section 15 of this act;

(2) Through the implementation of this chapter, protect the fundamental privacy rights of consumers with respect to the use of their personal data;

(3) Promote public awareness and understanding of risks, rules, responsibilities, safeguards, and rights in relation to the collection, use, sharing, and disclosure of personal data;

(4) Provide guidance to consumers regarding their rights under this chapter;

(5) Monitor relevant developments relating to the protection of personal data, and in particular, the development of information and communication technologies and commercial practices;

(6) Provide technical assistance and advice to the legislature, upon request, with respect to privacy-related legislation;

(7) Determine which controllers and processors have been newly established within the previous three years for the purposes of compliance with the registration and reporting requirements in section 13 of this act;

(8) Provide guidance, upon request, to controllers and processors regarding their obligations under this chapter;

(9) Encourage the formation of codes of conduct by controllers and processors and provide an opinion and approve those codes of conduct it deems to provide sufficient privacy safeguards;

(10) Establish a data protection certification mechanism, approving all criteria for such certification and data protection seals and marks to indicate such certification. The commission shall conduct periodic reviews of certifications issued, where applicable, and shall deny or withdraw certifications if the established criteria are not met or are no longer met by a controller or processor;

(11) Conduct data protection audits of controllers or processors upon a request from a controller or processor, or as the commission deems prudent and necessary; and

(12) Perform all other acts necessary and appropriate in the exercise of its power, authority, and jurisdiction and seek to balance the goals of strengthening consumer privacy while giving attention to the impact on businesses.

NEW SECTION. **Sec. 17.** POWERS OF THE WASHINGTON STATE CONSUMER DATA PRIVACY COMMISSION. (1) The commission may order a controller or processor to provide any information the commission requires for the performance of its duties, including access to a controller or processor's premises and data processing equipment and means.

(2) The commission may subpoena witnesses, compel their attendance, administer oaths, take the testimony of any person under oath, and require by subpoena the production of any books, papers, records, or other items material to the performance of the commission's duties or exercise of its powers including, but not limited to, its power to audit a controller or processor's compliance with this chapter and any rules adopted by the commission pursuant to section 15 of this act.

NEW SECTION. **Sec. 18.** ADMINISTRATIVE ENFORCEMENT. (1) Upon the complaint of a consumer or on its own initiative, the commission may investigate alleged violations by a controller or processor of this chapter or any rules issued by the commission. The commission may decide not to investigate a complaint. In making a decision not to investigate or provide more time to cure, the commission may consider the following:

(a) Lack of intent to violate this chapter or any rules issued by the commission; and

(b) Voluntary efforts undertaken by the controller or processor to cure the alleged violation prior to being notified by the commission of the complaint.

(2) The commission shall notify in writing the consumer who made the complaint of the action, if any, the commission has taken or plans to take on the complaint, together with the reasons for that action or nonaction.

(3)(a) The commission may not make a finding that there is reason to believe that a violation has occurred unless, at least 30 days prior to the commission's consideration of the alleged violation, the alleged violator is:

(i) Notified of the alleged violation by service of process or registered mail with return receipt requested;

(ii) Provided with a summary of the evidence; and

(iii) Informed of their right to be present in person and represented by counsel at any proceeding of the commission held for the purpose of considering whether there is reason to believe that a violation has occurred.

(b) Notice to the alleged violator is deemed made on the date of service, the date the registered mail receipt is signed, or if the registered mail receipt is not signed, the date returned by the post office.

(c) A proceeding held for the purpose of considering whether there is reason to believe that a violation has occurred is private unless the alleged violator files with the commission a written request that the proceeding be public.

(4)(a) If the commission determines there is reason to believe that this chapter or a rule adopted by the commission has been violated, prior to holding a hearing pursuant to subsection (5) of this section, the commission shall issue to the controller or processor a warning letter identifying specific provisions of this chapter the commission believes have been or are being violated.

(b) Within 30 days of the issuance of the warning letter, the controller or processor shall provide the commission with a written response to explain that the alleged violation has not been committed or to summarize how the violation has been cured.

(c) Upon the receipt of the controller or processor's response, the commission shall make a written finding as to whether a violation has been committed and whether the violation has been cured. If the commission finds that no violation has been committed, the commission shall close the matter. If the commission finds the violation has not been cured, the commission may proceed with the administrative hearing pursuant to subsection (5) of this section.

(5)(a) When the commission determines there is reason to believe that this chapter or a rule adopted by the commission has been violated and that the violation has not been cured pursuant to subsection (4) of this section, it shall hold a hearing to determine if a violation has occurred. Notice must be given and the hearing conducted in accordance with the administrative procedure act, chapter 34.05 RCW. The commission shall have all the powers granted by that chapter.

(b) If the commission determines on the basis of the hearing conducted pursuant to (a) of this subsection that a violation has occurred, the commission shall issue an order that may require the violator to do all or any of the following:

(i) Cease and desist the violation; or

(ii) Pay an administrative fine of up to $2,500 for each violation, or up to $7,500 for each intentional violation and each violation involving the personal data of a minor.

(c) All receipts from the imposition of administration fines under this subsection must be deposited into the consumer privacy account created in section 21 of this act.

(d) When the commission determines that no violation has occurred, it shall publish a declaration so stating.

(6) Any decision of the commission with respect to a complaint or administrative fine is subject to judicial review in an action brought by a party to the complaint or administrative fine and is subject to an abuse of discretion standard.

(7) Upon reviewing a complaint, the commission may refer the complaint to the attorney general for civil enforcement under the consumer protection act, chapter 19.86 RCW. The commission and the attorney general may consult prior to referral to determine the appropriate enforcement mechanism.

NEW SECTION. **Sec. 19.** ENFORCEMENT BY THE ATTORNEY GENERAL. (1) This chapter may be enforced by the attorney general under the consumer protection act, chapter 19.86 RCW.

(2) In actions brought by the attorney general, the legislature finds: (a) 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; and (b) a violation of this chapter is not reasonable in relation to the development and preservation of business, is an unfair or deceptive act in trade or commerce, and is an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW.

(3) The legislative declarations in this section do not apply to any claim or action by any party other than the attorney general alleging that conduct regulated by this chapter violates chapter 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

(4) Until July 31, 2024, in the event of a controller's or processor's violation under this chapter, prior to filing a complaint, the attorney general must provide the controller or processor with a warning letter identifying the specific provisions of this chapter the attorney general alleges have been or are being violated. If, after 30 days of issuance of the warning letter, the attorney general believes the controller or processor has failed to

cure any alleged violation, the attorney general may bring an action against the controller or processor as provided under this chapter.

(5) All receipts from the imposition of civil penalties under this section must be deposited into the consumer privacy account created in section 21 of this act.

(6) No action may be filed by the attorney general under this section for any violation of this chapter by a controller or processor after the commission has issued a decision pursuant to section 18 of this act against that controller or processor for the same violation.

NEW SECTION. **Sec. 20.** PRIVATE RIGHT OF ACTION. (1)(a) A person injured by a violation of this chapter may bring a civil action under the consumer protection act, chapter 19.86 RCW.

(b) The legislative declarations in section 19(2) of this act do not apply to any claim or action brought pursuant to this section.

(2)(a) Thirty days prior to filing an action pursuant to this section, a first party claimant shall provide written notice of the basis for the action to the defendant and the commission. Notice may be provided by email, regular mail, registered mail, or certified mail with return receipt requested. Proof of notice by mail may be made in the same manner as prescribed by court rule or statute for proof of service by mail. The defendant and the commission are deemed to have received notice three business days after the notice is mailed.

(b) If the defendant fails to resolve the basis for the action within the 30-day period after the written notice by the first party claimant, the claimant may bring the action without any further notice.

(c) If a written notice of action is served under (a) of this subsection within the time prescribed for the filing of an action under this section, the statute of limitations for the action is tolled during the 30-day period of time in (a) of this subsection.

(3) Nothing in this chapter limits any other independent causes of action enjoyed by any person, including any constitutional, statutory, administrative, or common law rights or causes of action. The rights and protections in this chapter are not exclusive, and to the extent that a person has the rights and protections in this chapter because of another law other than this chapter, the person

continues to have those rights and protections notwithstanding the existence of this chapter.

NEW SECTION. **Sec. 21.** CONSUMER PRIVACY ACCOUNT. The consumer privacy account is created in the state treasury. All receipts from the imposition of administrative fines and civil penalties under this chapter and the annual fee under section 24 of this act must be deposited into the account. Moneys in the account may be spent only after appropriation. Moneys in the account may only be used for the purposes of recovery of costs and attorneys' fees accrued by the attorney general in enforcing this chapter and for the commission. Moneys may not be used to supplant general fund appropriations to either agency.

NEW SECTION. **Sec. 22.** PREEMPTION. (1) Except as provided in this section, this chapter supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by any local entity regarding the processing of personal data by controllers or processors.

(2) Laws, ordinances, or regulations regarding the processing of personal data by controllers or processors that are adopted by any local entity prior to July 1, 2021, are not superseded or preempted.

NEW SECTION. **Sec. 23.** A new section is added to chapter 42.56 RCW to read as follows:

Data protection assessments submitted by a controller to the attorney general in accordance with requirements under section 11 of this act are exempt from disclosure under this chapter.

NEW SECTION. **Sec. 24.** DATA COLLECTION FEE ON DATA CONTROLLERS AND DATA PROCESSORS. (1) Notwithstanding any other provision of this chapter, or of any other law, beginning on or after January 1, 2023, an annual fee is imposed upon every data controller or data processor that is required to register with the commission pursuant to section 13 of this act.

(2) For the purposes of assessing the fee imposed by this section, the commission shall share with the department of revenue a complete directory of all data controllers and processors registered with the commission.

(3) All receipts from the imposition of the annual data collection fee under this section must be deposited into the consumer

privacy account created in section 21 of this act and may be used only for the operating expenses of the commission.

(4) This section does not apply to institutions of higher education.

NEW SECTION. **Sec. 25.** Sections 1 through 22 and 24 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. **Sec. 26.** Sections 1, 2, and 14 through 16 of this act take effect July 31, 2022.

NEW SECTION. **Sec. 27.** Sections 3 through 13 and 17 through 24 of this act take effect July 31, 2023.

NEW SECTION. **Sec. 28.** Sections 3 through 22 of this act do not apply to institutions of higher education until July 31, 2027.

NEW SECTION. **Sec. 29.** Sections 3 through 22 and 24 of this act do not apply to nonprofit corporations until July 31, 2027.

NEW SECTION. **Sec. 30.** 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.

--- END ---