

---

**HOUSE BILL 1850**

---

**State of Washington**

**67th Legislature**

**2022 Regular Session**

**By** Representatives Slatter, Berg, Pollet, Harris-Talley, and Corry

Prefiled 01/07/22. Read first time 01/10/22. Referred to Committee on Civil Rights & Judiciary.

1 AN ACT Relating to protecting and enforcing the foundational data  
2 privacy rights of Washingtonians; adding a new section to chapter  
3 42.56 RCW; adding a new chapter to Title 19 RCW; creating new  
4 sections; prescribing penalties; and providing an effective date.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

24 (5) "Child" has the same meaning as defined in the children's  
25 online privacy protection act, Title 15 U.S.C. Sec. 6501 through  
26 6506.

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

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

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

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

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

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

14 (12) "Decisions that produce legal effects concerning a consumer  
15 or similarly significant effects concerning a consumer" means  
16 decisions that result in the provision or denial of financial and  
17 lending services, housing, insurance, education enrollment, criminal  
18 justice, employment opportunities, health care services, or access to  
19 basic necessities, such as food and water.

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

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

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

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

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

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

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

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

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

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

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

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

14 (25) "Nonprofit corporation" has the same meaning as in RCW  
15 24.03.005.

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

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

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

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

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

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

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

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

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

12 (b) "Sharing" does not include the following: (i) The disclosure  
13 of personal data to a processor who processes the personal data on  
14 behalf of the controller; (ii) the disclosure of personal data to a  
15 third party with whom the consumer has a direct relationship for  
16 purposes of providing a product or service requested by the consumer;  
17 (iii) the disclosure or transfer of personal data to an affiliate of  
18 the controller; (iv) the disclosure of information that the consumer  
19 (A) intentionally made available to the general public via a channel  
20 of mass media, and (B) did not restrict to a specific audience; or  
21 (v) the disclosure or transfer of personal data to a third party as  
22 an asset that is part of a merger, acquisition, bankruptcy, or other  
23 transaction in which the third party assumes control of all or part  
24 of the controller's assets.

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

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

39 (36) "Targeted advertising" means displaying advertisements to a  
40 consumer where the advertisement is selected based on personal data

1 obtained from a consumer's activities over time and across one or  
2 more distinctly branded websites or online applications to predict  
3 the consumer's preferences or interests. It does not include  
4 advertising: (a) Based on activities within a controller's own  
5 commonly branded websites or online applications; (b) based on the  
6 context of a consumer's current search query or visit to a website or  
7 online application; or (c) to a consumer in response to the  
8 consumer's request for information or feedback.

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

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

16 (a) During a calendar year, control or process personal data of  
17 100,000 consumers or more; or

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

21 (2) This chapter does not apply to:

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

24 (b) Municipal corporations;

25 (c) Air carriers;

26 (d) Nonprofit organizations that:

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

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

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

32 (e) Information that meets the definition of:

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

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

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

1 (iv) Identifiable private information for purposes of the federal  
2 policy for the protection of human subjects, 45 C.F.R. Part 46;  
3 identifiable private information that is otherwise information  
4 collected as part of human subjects research pursuant to the good  
5 clinical practice guidelines issued by the international council for  
6 harmonization; the protection of human subjects under 21 C.F.R. Parts  
7 50 and 56; or personal data used or shared in research conducted in  
8 accordance with one or more of the requirements set forth in this  
9 subsection;

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

12 (A) A quality improvement committee for purposes of RCW  
13 43.70.510, 70.230.080, or 70.41.200;

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

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

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

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

24 (vii) Patient safety work product for purposes of 42 C.F.R. Part  
25 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26; or

26 (viii) Information that is (A) deidentified in accordance with  
27 the requirements for deidentification set forth in 45 C.F.R. Part  
28 164, and (B) derived from any of the health care-related information  
29 listed in this subsection (2)(e);

30 (f) Information originating from, and intermingled to be  
31 indistinguishable with, information under (e) of this subsection that  
32 is maintained by:

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

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

38 (iii) A program or a qualified service organization as defined by  
39 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;



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

3 (h)(i) An activity involving the collection, maintenance,  
4 disclosure, sharing, communication, or use of any personal data  
5 bearing on a consumer's credit worthiness, credit standing, credit  
6 capacity, character, general reputation, personal characteristics, or  
7 mode of living by a consumer reporting agency, as defined in Title 15  
8 U.S.C. Sec. 1681a(f), by a furnisher of information, as set forth in  
9 Title 15 U.S.C. Sec. 1681s-2, who provides information for use in a  
10 consumer report, as defined in Title 15 U.S.C. Sec. 1681a(d), and by  
11 a user of a consumer report, as set forth in Title 15 U.S.C. Sec.  
12 1681b.

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

20 (i) Personal data collected and maintained for purposes of  
21 chapter 43.71 RCW;

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

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

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

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

35 (n) Personal data collected, maintained, disclosed, or otherwise  
36 used in connection with the gathering, dissemination, or reporting of  
37 news or information to the public by news media as defined in RCW  
38 5.68.010(5);

39 (o) Personal data collected, processed, shared, or disclosed  
40 pursuant to the federal farm credit act of 1971 (as amended in 12

1 U.S.C. Sec. 2001-2279cc) and its implementing regulations (12 C.F.R.  
2 Part 600 et seq.) if the collection, processing, sharing, or  
3 disclosure is in compliance with that law; or

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

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

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

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

25 (2) A consumer has the right to correct inaccurate personal data  
26 concerning the consumer, taking into account the nature of the  
27 personal data and the purposes of the processing of the personal  
28 data.

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

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

38 (5) A consumer has the right to opt out of the processing of  
39 personal data concerning such a consumer for the purposes of (a)

1 targeted advertising; (b) the sharing of personal data; or (c)  
2 profiling in furtherance of decisions that produce legal effects  
3 concerning a consumer or similarly significant effects concerning a  
4 consumer.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

35 (b) Taking into account the nature of processing and the  
36 information available to the processor, the processor shall: Assist  
37 the controller in meeting the controller's obligations in relation to  
38 the security of processing the personal data and in relation to the  
39 notification of a breach of the security of the system pursuant to

1 RCW 19.255.010; and provide information to the controller necessary  
2 to enable the controller to conduct and document any data protection  
3 assessments required by section 11 of this act. The controller and  
4 processor are each responsible for only the measures allocated to  
5 them.

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

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

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

15 (4) Taking into account the context of processing, the controller  
16 and the processor shall implement appropriate technical and  
17 organizational measures to ensure a level of security appropriate to  
18 the risk and establish a clear allocation of the responsibilities  
19 between them to implement such measures.

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

29 (a) At the choice of the controller, the processor shall delete  
30 or return all personal data to the controller as requested at the end  
31 of the provision of services, unless retention of the personal data  
32 is required by law;

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

36 (ii) The processor shall allow for, and contribute to, reasonable  
37 audits and inspections by the controller or the controller's  
38 designated auditor. Alternatively, the processor may, with the  
39 controller's consent, arrange for a qualified and independent auditor  
40 to conduct, at least annually and at the processor's expense, an

1 audit of the processor's policies and technical and organizational  
2 measures in support of the obligations under this chapter using an  
3 appropriate and accepted control standard or framework and audit  
4 procedure for the audits as applicable, and provide a report of the  
5 audit to the controller upon request.

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

9 (7) Determining whether a person is acting as a controller or  
10 processor with respect to a specific processing of data is a fact-  
11 based determination that depends upon the context in which personal  
12 data are to be processed. A person that is not limited in its  
13 processing of personal data pursuant to a controller's instructions,  
14 or that fails to adhere to such instructions, is a controller and not  
15 a processor with respect to a specific processing of data. A  
16 processor that continues to adhere to a controller's instructions  
17 with respect to a specific processing of personal data remains a  
18 processor. If a processor begins, alone or jointly with others,  
19 determining the purposes and means of the processing of personal  
20 data, it is a controller with respect to the processing.

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

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

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

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

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

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

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

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

1 (i) Use clear and plain language;

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

4 (iii) Be understandable to the least sophisticated consumer.

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

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

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

15 (5) A controller shall establish, implement, and maintain  
16 reasonable administrative, technical, and physical data security  
17 practices to protect the confidentiality, integrity, and  
18 accessibility of personal data. The data security practices must be  
19 appropriate to the volume and nature of the personal data at issue.

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

29 (7) A controller may not discriminate against a consumer for  
30 exercising any of the rights contained in this chapter, including  
31 denying goods or services to the consumer, charging different prices  
32 or rates for goods or services, and providing a different level of  
33 quality of goods and services to the consumer. This subsection does  
34 not prohibit a controller from offering a different price, rate,  
35 level, quality, or selection of goods or services to a consumer,  
36 including offering goods or services for no fee, if the offering is  
37 in connection with a consumer's voluntary participation in a bona  
38 fide loyalty, rewards, premium features, discounts, or club card  
39 program. If a consumer exercises their right pursuant to section 5(5)  
40 of this act, a controller may not share personal data with a third-



1 party controller as part of such a program unless: (a) The sharing is  
2 reasonably necessary to enable the third party to provide a benefit  
3 to which the consumer is entitled; (b) the sharing of personal data  
4 to third parties is clearly disclosed in the terms of the program;  
5 and (c) the third party uses the personal data only for purposes of  
6 facilitating such a benefit to which the consumer is entitled and  
7 does not retain or otherwise use or disclose the personal data for  
8 any other purpose.

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

15 (b) A controller shall provide an effective mechanism for a  
16 consumer to revoke consent after it is given. After a consumer  
17 revokes consent, the controller shall cease processing the consumer's  
18 sensitive data as soon as practicable, but in no case any later than  
19 15 days after the consumer's revocation of consent.

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

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

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

32 (a) Reidentify deidentified data;

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

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

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

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

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

12 (2) The rights contained in section 5 (1) through (4) of this act  
13 do not apply to pseudonymous data in cases where the controller is  
14 able to demonstrate any information necessary to identify the  
15 consumer is kept separately and is subject to effective technical and  
16 organizational controls that prevent the controller from accessing  
17 such information.

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

23 NEW SECTION. **Sec. 11.** DATA PROTECTION ASSESSMENTS. (1)

24 Controllers must conduct and document a data protection assessment of  
25 each of the following processing activities involving personal data:

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

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

30 (c) The processing of personal data for purposes of profiling,  
31 where such profiling presents a reasonably foreseeable risk of: (i)  
32 Unfair or deceptive treatment of, or disparate impact on, consumers;  
33 (ii) financial, physical, or reputational injury to consumers; (iii)  
34 a physical or other intrusion upon the solitude or seclusion, or the  
35 private affairs or concerns, of consumers, where such intrusion would  
36 be offensive to a reasonable person; or (iv) other substantial injury  
37 to consumers;

38 (d) The processing of sensitive data; and

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

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

7 (2) Data protection assessments conducted under subsection (1) of  
8 this section must identify and weigh the benefits that may flow  
9 directly and indirectly from the processing to the controller,  
10 consumer, other stakeholders, and the public against the potential  
11 risks to the rights of the consumer associated with such processing,  
12 as mitigated by safeguards that can be employed by the controller to  
13 reduce such risks. The use of deidentified data and the reasonable  
14 expectations of consumers, as well as the context of the processing  
15 and the relationship between the controller and the consumer whose  
16 personal data will be processed, must be factored into this  
17 assessment by the controller.

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

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

37 NEW SECTION. **Sec. 12.** LIMITATIONS AND APPLICABILITY. (1) The  
38 obligations imposed on controllers or processors under this chapter  
39 do not restrict a controller's or processor's ability to do any of

1 the following, to the extent that the processing of a consumer's  
2 personal data is reasonably necessary and proportionate for these  
3 purposes:

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

6 (b) Comply with a civil, criminal, or regulatory inquiry,  
7 investigation, subpoena, or summons by federal, state, local, or  
8 other governmental authorities;

9 (c) Cooperate with law enforcement agencies concerning conduct or  
10 activity that the controller or processor reasonably and in good  
11 faith believes may violate federal, state, or local laws, rules, or  
12 regulations;

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

15 (e) Provide a product or service specifically requested by a  
16 consumer, perform a contract to which the consumer is a party, or  
17 take steps at the request of the consumer prior to entering into a  
18 contract;

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

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

27 (h) Engage in public or peer-reviewed scientific, historical, or  
28 statistical research in the public interest that adheres to all other  
29 applicable ethics and privacy laws and is approved, monitored, and  
30 governed by an institutional review board, human subjects research  
31 ethics review board, or a similar independent oversight entity that  
32 determines: (i) If the research is likely to provide substantial  
33 benefits that do not exclusively accrue to the controller; (ii) the  
34 expected benefits of the research outweigh the privacy risks; and  
35 (iii) if the controller has implemented reasonable safeguards to  
36 mitigate privacy risks associated with research, including any risks  
37 associated with reidentification; or

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

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

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

6 (b) Perform solely internal operations that are reasonably  
7 aligned with the expectations of the consumer based on the consumer's  
8 existing relationship with the controller, or are otherwise  
9 compatible with processing in furtherance of the provision of a  
10 product or service specifically requested by a consumer or the  
11 performance of a contract to which the consumer is a party when those  
12 internal operations are performed during, and not following, the  
13 consumer's relationship with the controller.

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

21 (4) A controller or processor that discloses personal data to a  
22 third-party controller or processor in compliance with the  
23 requirements of this chapter is not in violation of this chapter if  
24 the recipient processes such personal data in violation of this  
25 chapter, provided that, at the time of disclosing the personal data,  
26 the disclosing controller or processor did not have actual knowledge  
27 that the recipient intended to commit a violation. A third-party  
28 controller or processor receiving personal data from a controller or  
29 processor in compliance with the requirements of this chapter is  
30 likewise not in violation of this chapter for the obligations of the  
31 controller or processor from which it receives such personal data.

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

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

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

39 (6) Processing personal data solely for the purposes expressly  
40 identified in subsection (1)(a) through (g) of this section does not,

1 by itself, make an entity a controller with respect to the  
2 processing.

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

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

10 (b) Personal data that is processed by a controller pursuant to  
11 this section may be processed solely to the extent that such  
12 processing is: (i) Necessary, reasonable, and proportionate to the  
13 purposes listed in this section; (ii) adequate, relevant, and limited  
14 to what is necessary in relation to the specific purpose or purposes  
15 listed in this section; and (iii) insofar as possible, taking into  
16 account the nature and purpose of processing the personal data,  
17 subjected to reasonable administrative, technical, and physical  
18 measures to protect the confidentiality, integrity, and accessibility  
19 of the personal data, and to reduce reasonably foreseeable risks of  
20 harm to consumers.

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

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

28 (b) Provide the following information to the commission:

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

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

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

36 (iv) A statement specifying the amount of personal data  
37 collected, processed, or shared globally in the preceding year;

1 (v) A statement specifying the amount of personal data of  
2 Washington consumers collected, processed, or shared in the preceding  
3 year; and

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

5 (c) Pay a registration fee equal to:

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

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

10 (2) A controller or processor that fails to register as required  
11 by subsection (1)(a) of this section is subject to a fine between  
12 \$1,000 and \$20,000 for each day it fails to register pursuant to this  
13 section.

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

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

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

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

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

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

36 (d) The commission may employ staff as necessary to carry out the  
37 commission's duties as prescribed in this chapter. The Washington  
38 utilities and transportation commission shall provide all  
39 administrative staff support for the commission, which shall

1 otherwise retain its independence in exercising its powers,  
2 functions, and duties and its supervisory control over  
3 nonadministrative staff.

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

- 10 (i) Adopt, amend, or rescind rules;
  - 11 (ii) Determine that a violation of this chapter has occurred; or
  - 12 (iii) Assess penalties for violations.
- 13 (2) Members of the commission shall:
- 14 (a) Have qualifications, experience, and skills, in particular in  
15 the areas of privacy and technology, required to perform the duties  
16 of the commission and exercise its powers and authority;
  - 17 (b) Maintain the confidentiality of information that has come to  
18 their knowledge in the course of the performance of their tasks or  
19 exercise of their powers, except to the extent that disclosure is  
20 required by chapter 42.56 RCW;
  - 21 (c) Remain free from external influence, whether direct or  
22 indirect, and neither seek nor take instructions from another;
  - 23 (d) Refrain from any action incompatible with their duties or  
24 engage in any incompatible occupation, whether gainful or not, during  
25 their term;
  - 26 (e) Have the right of access to all information made available by  
27 the commission to the chair of the commission;
  - 28 (f) Be precluded, for a period of one year after leaving office,  
29 from accepting employment with a controller or processor that was  
30 subject to an enforcement action or civil action under this chapter  
31 during the member's tenure or during the five-year period preceding  
32 the member's appointment; and
  - 33 (g) Be precluded for a period of two years after leaving office  
34 from acting, for compensation, as an agent or attorney for, or  
35 otherwise representing, any other person in a matter pending before  
36 the commission if the purpose is to influence an action of the  
37 commission.

38 NEW SECTION. **Sec. 15.** RULE-MAKING AUTHORITY OF THE WASHINGTON  
39 STATE CONSUMER DATA PRIVACY COMMISSION. The commission shall adopt,



1 amend, and rescind suitable rules under the administrative procedure  
2 act, chapter 34.05 RCW, to carry out the purposes and provisions of  
3 this chapter, and the policies and practices of the commission in  
4 connection therewith.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20 (4) (a) When the commission determines there is reason to believe  
21 that this chapter or a rule adopted by the commission has been  
22 violated, it shall hold a hearing to determine if a violation has  
23 occurred. Notice must be given and the hearing conducted in  
24 accordance with the administrative procedure act, chapter 34.05 RCW.  
25 The commission shall have all the powers granted by that chapter.

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

30 (i) Cease and desist the violation; or

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

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

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

39 (5) Any decision of the commission with respect to a complaint or  
40 administrative fine is subject to judicial review in an action

1 brought by a party to the complaint or administrative fine and is  
2 subject to an abuse of discretion standard.

3 (6) The commission may refer a complaint to the attorney general  
4 when the commission believes additional authority is needed to ensure  
5 full compliance with this chapter.

6 (7) The commission shall, upon request by the attorney general,  
7 stay an administrative action or investigation under this chapter to  
8 permit the attorney general to proceed with an investigation or civil  
9 action, and shall not pursue an administrative action or  
10 investigation unless the attorney general subsequently determines not  
11 to pursue an investigation or civil action. The commission may not  
12 limit the authority of the attorney general to enforce this chapter.

13 NEW SECTION. **Sec. 19.** ENFORCEMENT BY THE ATTORNEY GENERAL. (1)

14 This chapter may be enforced by the attorney general under the  
15 consumer protection act, chapter 19.86 RCW.

16 (2) In actions brought by the attorney general, the legislature  
17 finds: (a) The practices covered by this chapter are matters vitally  
18 affecting the public interest for the purpose of applying the  
19 consumer protection act, chapter 19.86 RCW; and (b) a violation of  
20 this chapter is not reasonable in relation to the development and  
21 preservation of business, is an unfair or deceptive act in trade or  
22 commerce, and is an unfair method of competition for the purpose of  
23 applying the consumer protection act, chapter 19.86 RCW.

24 (3) The legislative declarations in this section do not apply to  
25 any claim or action by any party other than the attorney general  
26 alleging that conduct regulated by this chapter violates chapter  
27 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

28 (4) Until July 31, 2023, in the event of a controller's or  
29 processor's violation under this chapter, prior to filing a  
30 complaint, the attorney general must provide the controller or  
31 processor with a warning letter identifying the specific provisions  
32 of this chapter the attorney general alleges have been or are being  
33 violated. If, after 30 days of issuance of the warning letter, the  
34 attorney general believes the controller or processor has failed to  
35 cure any alleged violation, the attorney general may bring an action  
36 against the controller or processor as provided under this chapter.

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

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

6 NEW SECTION. **Sec. 20.** PRIVATE RIGHT OF ACTION. (1) A person  
7 injured by a violation of this chapter may bring a civil action in  
8 superior court to enjoin further violations and to recover actual  
9 damages. For purposes of this section, "actual damages" means:

10 (a) The demonstrable economic value to the injured person of  
11 exclusive control of the personal data processed in violation of this  
12 chapter, or the economic value to the controller or processor of the  
13 personal data processed in violation of this chapter, whichever is  
14 greater; and

15 (b) The amount necessary to compensate the person for  
16 reputational harm and emotional distress resulting from the  
17 violation.

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

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

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

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

1 chapter because of another law other than this chapter, the person  
2 continues to have those rights and protections notwithstanding the  
3 existence of this chapter.

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

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

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

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

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

26 NEW SECTION. **Sec. 24.** DATA COLLECTION FEE ON DATA CONTROLLERS  
27 AND DATA PROCESSORS. (1) Notwithstanding any other provision of this  
28 chapter, or of any other law, beginning on or after January 1, 2023,  
29 an annual fee is imposed upon every data controller or data processor  
30 that is required to register with the commission pursuant to section  
31 13 of this act.

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

1 (3) All receipts from the imposition of the annual data  
2 collection fee under this section must be deposited into the consumer  
3 privacy account created in section 21 of this act and may be used  
4 only for the operating expenses of the commission.

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

7 NEW SECTION. **Sec. 25.** Sections 1 through 22, 24, and 26 of this  
8 act constitute a new chapter in Title 19 RCW.

9 NEW SECTION. **Sec. 26.** Sections 1 through 24 of this act take  
10 effect July 31, 2022.

11 NEW SECTION. **Sec. 27.** Sections 3 through 22 of this act do not  
12 apply to institutions of higher education until July 31, 2027.

13 NEW SECTION. **Sec. 28.** Sections 3 through 22 and 24 of this act  
14 do not apply to nonprofit corporations until July 31, 2027.

15 NEW SECTION. **Sec. 29.** If any provision of this act or its  
16 application to any person or circumstance is held invalid, the  
17 remainder of the act or the application of the provision to other  
18 persons or circumstances is not affected.

--- END ---