

---

**BILL REQUEST - CODE REVISER'S OFFICE**

---

BILL REQ. #: S-4873.3/20 3rd draft

ATTY/TYPIST: JO:eab

BRIEF DESCRIPTION: Concerning the management and oversight of  
personal data.

1 AN ACT Relating to the management and oversight of personal data;  
2 adding a new chapter to Title 19 RCW; prescribing penalties; and  
3 providing an effective date.

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

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

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

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

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

5 (3) Given that technological innovation and new uses of data can  
6 help solve societal problems and improve quality of life, the  
7 legislature seeks to shape responsible public policies where  
8 innovation and protection of individual privacy coexist. The  
9 legislature notes that our federal authorities have not developed or  
10 adopted into law regulatory or legislative solutions that give  
11 consumers control over their privacy. In contrast, the European  
12 Union's general data privacy regulation has continued to influence  
13 data privacy policies and practices of those businesses competing in  
14 global markets. In the absence of federal standards, Washington and  
15 other states across the United States are analyzing elements of the  
16 European Union's general data privacy regulation to enact state-based  
17 data privacy regulatory protections.

18 (4) With this act, Washington state will be among the first tier  
19 of states giving consumers the ability to protect their own rights to  
20 privacy and requiring companies to be responsible custodians of data  
21 as technological innovations emerge. This act does so by explicitly  
22 providing consumers the right to access, correction, and deletion of  
23 personal data, as well as the right to opt out of the collection and  
24 use of personal data for certain purposes. These rights will add to,  
25 and not subtract from, the consumer protection rights that consumers  
26 already have under Washington state law.

27 (5) Additionally, this act imposes affirmative obligations upon  
28 companies to safeguard personal data and provide clear,  
29 understandable, and transparent information to consumers about how  
30 their personal data are used. It strengthens compliance and  
31 accountability by requiring data protection assessments in the  
32 collection and use of personal data. Finally, it empowers the state  
33 attorney general to obtain and evaluate a company's data protection  
34 assessments, to impose penalties where violations occur, and to  
35 prevent against future violations.

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

1 (1) "Affiliate" means a legal entity that shares common branding  
2 with another legal entity and that controls, is controlled by, or is  
3 under common control with, that other legal entity. For these  
4 purposes, "control" or "controlled" means ownership of, or the power  
5 to vote, more than fifty percent of the outstanding shares of any  
6 class of voting security of a company; control in any manner over the  
7 election of a majority of the directors or of individuals exercising  
8 similar functions; or the power to exercise a controlling influence  
9 over the management of a company.

10 (2) "Authenticate" means to use reasonable means to determine  
11 that a request to exercise any of the rights in section 6 (1) through  
12 (5) of this act is being made by the consumer who is entitled to  
13 exercise such rights.

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

17 (4) "Child" means any natural person under thirteen years of age.

18 (5) "Consent" means a clear affirmative act signifying a freely  
19 given, specific, informed, and unambiguous indication of a consumer's  
20 agreement to the processing of personal data relating to the  
21 consumer, such as by a written statement, including by electronic  
22 means, or other clear affirmative action.

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

27 (7) "Controller" means the natural or legal person which, alone  
28 or jointly with others, determines the purposes and means of the  
29 processing of personal data.

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

33 (9) "Decisions that produce legal effects concerning a consumer  
34 or similarly significant effects concerning a consumer" means  
35 decisions that include, but are not limited to, the denial of  
36 consequential services or support, such as financial and lending  
37 services, housing, insurance, education enrollment, criminal justice,  
38 employment opportunities, health care services, and access to basic  
39 necessities, such as food and water.

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

10 (11) "Enroll," "enrolled," or "enrolling" means the process by  
11 which a facial recognition service creates a facial template from one  
12 or more images of a consumer and adds the facial template to a  
13 gallery used by the facial recognition service for identification,  
14 verification, or persistent tracking of consumers. It also includes  
15 the act of adding an existing facial template directly into a gallery  
16 used by a facial recognition service.

17 (12) "Facial recognition service" means technology that analyzes  
18 facial features and is used for the identification, verification, or  
19 persistent tracking of consumers in still or video images.

20 (13) "Facial template" means the machine-interpretable pattern of  
21 facial features that is extracted from one or more images of a  
22 consumer by a facial recognition service.

23 (14) "Health care facility" has the same meaning as in RCW  
24 70.02.010.

25 (15) "Health care information" has the same meaning as in RCW  
26 70.02.010.

27 (16) "Health care provider" has the same meaning as in RCW  
28 70.02.010.

29 (17) "Identification" means the use of a facial recognition  
30 service by a controller to determine whether an unknown consumer  
31 matches any consumer who has been enrolled in a gallery used by the  
32 facial recognition service.

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

35 (19) "Meaningful human review" means review or oversight by one  
36 or more individuals who are trained in accordance with section 18(9)  
37 of this act and who have the authority to alter the decision under  
38 review.

39 (20) "Ongoing surveillance" means tracking the physical movements  
40 of a specified individual through one or more public places over

1 time, whether in real time or through application of a facial  
2 recognition service to historical records. It does not include a  
3 single recognition or attempted recognition of an individual if no  
4 attempt is made to subsequently track that individual's movement over  
5 time after the individual has been recognized.

6 (21) "Persistent tracking" means the use of a facial recognition  
7 service to track the movements of a consumer on a persistent basis  
8 without recognition of that consumer. Such tracking becomes  
9 persistent as soon as:

10 (a) The facial template that permits the tracking uses a facial  
11 recognition service for more than forty-eight hours after the first  
12 enrolling of that template; or

13 (b) The data created by the facial recognition service are linked  
14 to any other data such that the consumer who has been tracked is  
15 identified or identifiable.

16 (22)(a) "Personal data" means any information that is linked or  
17 reasonably linkable to an identified or identifiable natural person.  
18 "Personal data" does not include deidentified data or publicly  
19 available information.

20 (b) For purposes of this subsection, "publicly available  
21 information" means information that is lawfully made available from  
22 federal, state, or local government records.

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

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

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

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

38 (27) "Pseudonymous data" means personal data that cannot be  
39 attributed to a specific natural person without the use of additional  
40 information, provided that such additional information is kept

1 separately and is subject to appropriate technical and organizational  
2 measures to ensure that the personal data are not attributed to an  
3 identified or identifiable natural person.

4 (28) "Recognition" means the use of a facial recognition service  
5 to determine whether:

6 (a) An unknown consumer matches any consumer who has been  
7 enrolled in a gallery used by the facial recognition service; or

8 (b) An unknown consumer matches a specific consumer who has been  
9 enrolled in a gallery used by the facial recognition service.

10 (29)(a) "Sale," "sell," or "sold" means the exchange of personal  
11 data for monetary or other valuable consideration by the controller  
12 to a third party.

13 (b) "Sale" does not include the following: (i) The disclosure of  
14 personal data to a processor who processes the personal data on  
15 behalf of the controller; (ii) the disclosure of personal data to a  
16 third party with whom the consumer has a direct relationship for  
17 purposes of providing a product or service requested by the consumer  
18 or otherwise in a manner that is consistent with a consumer's  
19 reasonable expectations considering the context in which the consumer  
20 provided the personal data to the controller; (iii) the disclosure or  
21 transfer of personal data to an affiliate of the controller; or (iv)  
22 the disclosure or transfer of personal data to a third party as an  
23 asset that is part of a merger, acquisition, bankruptcy, or other  
24 transaction in which the third party assumes control of all or part  
25 of the controller's assets.

26 (30) "Security or safety purpose" means physical security,  
27 protection of consumer data, safety, fraud prevention, or asset  
28 protection.

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

36 (32) "Serious criminal offense" means any felony under chapter  
37 9.94A RCW or an offense enumerated by Title 18 U.S.C. Sec. 2516.

38 (33) "Specific geolocation data" means information that directly  
39 identifies the specific location of a natural person with the  
40 precision and accuracy below one thousand seven hundred fifty feet.

1 (34) "Targeted advertising" means displaying advertisements to a  
2 consumer where the advertisement is selected based on personal data  
3 obtained from a consumer's activities over time and across  
4 nonaffiliated web sites or online applications to predict such  
5 consumer's preferences or interests. It does not include advertising:  
6 (a) Based on activities within a controller's own web sites or online  
7 applications; (b) based on the context of a consumer's current search  
8 query or visit to a web site or online application; or (c) to a  
9 consumer in response to the consumer's request for information or  
10 feedback.

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

14 (36) "Verification" means the use of a facial recognition service  
15 by a controller to determine whether a consumer is a specific  
16 consumer enrolled in a gallery used by the facial recognition  
17 service.

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

22 (a) Controls or processes personal data of one hundred thousand  
23 consumers or more; or

24 (b) Derives over fifty percent of gross revenue from the sale of  
25 personal data and processes or controls personal data of twenty-five  
26 thousand consumers or more.

27 (2) This chapter does not apply to:

28 (a) State and local governments;

29 (b) Municipal corporations;

30 (c) Information that meets the definition of:

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

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

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

37 (iv) Identifiable private information for purposes of the federal  
38 policy for the protection of human subjects, 45 C.F.R. Part 46, or  
39 identifiable private information that is otherwise information



1 collected as part of human subjects research pursuant to the good  
2 clinical practice guidelines issued by the international council for  
3 harmonisation, or the protection of human subjects under 21 C.F.R.  
4 Parts 50 and 56;

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

7 (A) A quality improvement committee for purposes of RCW  
8 43.70.510, 70.230.080, or 70.41.200;

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

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

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

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

19 (vii) Patient safety work product for purposes of 42 C.F.R. Part  
20 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26;

21 (d) Information originating from, and intermingled to be  
22 indistinguishable with, information under (c) of this subsection that  
23 is maintained by:

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

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

29 (iii) A program or a qualified service organization as defined by  
30 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

31 (e) An activity involving the collection, maintenance,  
32 disclosure, sale, communication, or use of any personal information  
33 bearing on a consumer's credit worthiness, credit standing, credit  
34 capacity, character, general reputation, personal characteristics, or  
35 mode of living by a consumer reporting agency, as defined in Title 15  
36 U.S.C. Sec. 1681a(f), by a furnisher of information, as set forth in  
37 Title 15 U.S.C. Sec. 1681s-2, who provides information for use in a  
38 consumer report, as defined in Title 15 U.S.C. Sec. 1681a(d), and by  
39 a user of a consumer report, as set forth in Title 15 U.S.C. Sec.  
40 1681b.

1 Such activity involving the collection, maintenance, disclosure,  
2 sale, communication, or use of such information by that agency,  
3 furnisher, or user is subject to regulation under the fair credit  
4 reporting act, Title 15 U.S.C. Sec. 1681 et seq., and the information  
5 may not be used, communicated, disclosed, or sold except as  
6 authorized by the fair credit reporting act;

7 (f) Personal data collected and maintained for purposes of  
8 chapter 43.71 RCW;

9 (g) Personal data collected, processed, sold, or disclosed  
10 pursuant to the federal Gramm-Leach-Bliley act (P.L. 106-102), and  
11 implementing regulations, if the collection, processing, sale, or  
12 disclosure is in compliance with that law;

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

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

22 (j) Personal data regulated by the federal family educations  
23 rights and privacy act, 20 U.S.C. Sec. 1232g and its implementing  
24 regulations;

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

27 (l) Data maintained for employment records purposes.

28 NEW SECTION. **Sec. 5.** RESPONSIBILITY ACCORDING TO ROLE. (1)

29 Controllers and processors are responsible for meeting their  
30 respective obligations established under this chapter.

31 (2) Processors are responsible under this chapter for adhering to  
32 the instructions of the controller and assisting the controller to  
33 meet its obligations under this chapter. Such assistance shall  
34 include the following:

35 (a) Taking into account the nature of the processing, the  
36 processor shall assist the controller by appropriate technical and  
37 organizational measures, insofar as this is possible, for the  
38 fulfillment of the controller's obligation to respond to consumer

1 requests to exercise their rights pursuant to section 6 of this act;  
2 and

3 (b) Taking into account the nature of processing and the  
4 information available to the processor, the processor shall assist  
5 the controller in meeting the controller's obligations in relation to  
6 the security of processing the personal data and in relation to the  
7 notification of a breach of the security of the system pursuant to  
8 RCW 19.255.010; and shall provide information to the controller  
9 necessary to enable the controller to conduct and document any data  
10 protection assessments required by section 9 of this act.

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

13 (a) Implement and maintain reasonable security procedures and  
14 practices to protect personal data, taking into account the context  
15 in which the personal data are to be processed;

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

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

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

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

36 (b) (i) The processor shall make available to the controller all  
37 information necessary to demonstrate compliance with the obligations  
38 in this chapter; and (ii) the processor shall allow for, and  
39 contribute to, reasonable audits and inspections by the controller or  
40 the controller's designated auditor; alternatively, the processor

1 shall arrange for a qualified and independent auditor to conduct, at  
2 least annually and at the processor's expense, an audit of the  
3 processor's policies and technical and organizational measures in  
4 support of the obligations under this chapter using an appropriate  
5 and accepted control standard or framework and audit procedure for  
6 such audits as applicable, and shall provide a report of such audit  
7 to the controller upon request.

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

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

21 NEW SECTION. **Sec. 6.** CONSUMER PERSONAL DATA RIGHTS. Consumers  
22 may exercise the rights set forth in this section by submitting a  
23 request, at any time, to a controller specifying which rights the  
24 consumer wishes to exercise. In the case of processing personal data  
25 concerning a known child, the parent or legal guardian of the known  
26 child shall exercise the rights of this chapter on the child's  
27 behalf. Except as provided in this chapter, the controller must  
28 comply with a request to exercise the rights pursuant to subsections  
29 (1) through (5) of this section.

30 (1) *Right of access.* A consumer has the right to confirm whether  
31 or not a controller is processing personal data concerning the  
32 consumer and access such personal data.

33 (2) *Right to correction.* A consumer has the right to correct  
34 inaccurate personal data concerning the consumer, taking into account  
35 the nature of the personal data and the purposes of the processing of  
36 the personal data.

37 (3) *Right to deletion.* A consumer has the right to delete  
38 personal data concerning the consumer.

1           (4) *Right to data portability.* When exercising the right to  
2 access personal data pursuant to subsection (1) of this section, a  
3 consumer has the right to obtain personal data concerning the  
4 consumer, which the consumer previously provided to the controller,  
5 in a portable and, to the extent technically feasible, readily usable  
6 format that allows the consumer to transmit the data to another  
7 controller without hindrance, where the processing is carried out by  
8 automated means.

9           (5) *Right to opt out.* A consumer has the right to opt out of the  
10 processing of personal data concerning such consumer for purposes of  
11 targeted advertising, the sale of personal data, or profiling in  
12 furtherance of decisions that produce legal effects concerning a  
13 consumer or similarly significant effects concerning a consumer.

14           (6) *Notifying third parties of consumer requests.* A controller  
15 must, upon request, take reasonable steps to communicate a consumer's  
16 request to correct, delete, or opt out of the processing of personal  
17 data under subsection (2), (3), or (5) of this section to each third  
18 party to whom the controller disclosed the personal data within one  
19 year preceding the consumer's request, unless this proves  
20 functionally impractical, technically infeasible, or involves  
21 disproportionate effort.

22           (7) *Responding to consumer requests.* (a) A controller must inform  
23 a consumer of any action taken on a request under subsections (1)  
24 through (5) of this section without undue delay and in any event  
25 within forty-five days of receipt of the request. That period may be  
26 extended once by forty-five additional days where reasonably  
27 necessary, taking into account the complexity and number of the  
28 requests. The controller must inform the consumer of any such  
29 extension within forty-five days of receipt of the request, together  
30 with the reasons for the delay.

31           (b) If a controller does not take action on the request of a  
32 consumer, the controller must inform the consumer without undue delay  
33 and at the latest within thirty days of receipt of the request of the  
34 reasons for not taking action and instructions for how to appeal the  
35 decision with the controller as described in subsection (8) of this  
36 section.

37           (c) Information provided under this section must be provided by  
38 the controller free of charge, up to twice annually to the consumer.  
39 Where requests from a consumer are manifestly unfounded or excessive,  
40 in particular because of their repetitive character, the controller

1 may either: (i) Charge a reasonable fee to cover the administrative  
2 costs of complying with the request, or (ii) refuse to act on the  
3 request. The controller bears the burden of demonstrating the  
4 manifestly unfounded or excessive character of the request.

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

11 (8)(a) Controllers must establish an internal process whereby  
12 consumers may appeal a refusal to take action on a request to  
13 exercise any of the rights under subsections (1) through (5) of this  
14 section within a reasonable period of time after the consumer's  
15 receipt of the notice sent by the controller under subsection (7)(b)  
16 of this section.

17 (b) The appeal process must be conspicuously available and as  
18 easy to use as the process for submitting such requests under this  
19 section.

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

34 (d) When informing a consumer of any action taken or not taken in  
35 response to an appeal pursuant to (c) of this subsection, the  
36 controller must clearly and prominently ask the consumer whether the  
37 consumer consents to having the controller submit the appeal, along  
38 with any action taken or not taken by the controller in response to  
39 the appeal and the controller's written explanation of the reasons in  
40 support thereof, to the attorney general. If the consumer provides

1 such consent, the controller must submit such information to the  
2 attorney general.

3 (e) The attorney general must make publicly available on its web  
4 site all information it receives from a controller pursuant to (d) of  
5 this subsection, except that any information that may identify a  
6 consumer shall be redacted from such information before it is made  
7 publicly available on the attorney general's web site.

8 NEW SECTION. **Sec. 7.** PROCESSING DEIDENTIFIED DATA OR  
9 PSEUDONYMOUS DATA. (1) This chapter does not require a controller or  
10 processor to do any of the following solely for purposes of complying  
11 with this chapter:

12 (a) Reidentify deidentified data;  
13 (b) Comply with an authenticated consumer request to access,  
14 correct, delete, or port personal data pursuant to section 6 (1)  
15 through (4) of this act, if all of the following are true:

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

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

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

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

31 (2) The rights contained in section 6 (1) through (4) of this act  
32 do not apply to pseudonymous data in cases where the controller is  
33 able to demonstrate that it is not in a position to identify the  
34 consumer, for instance, due to the institution of effective technical  
35 and organizational controls that prevent the controller from  
36 accessing information that would enable the identification of the  
37 consumer.

38 (3) A controller that uses pseudonymous data or deidentified data  
39 must exercise reasonable oversight to monitor compliance with any

1 contractual commitments to which the pseudonymous data or  
2 deidentified data are subject, and must take appropriate steps to  
3 address any breaches of contractual commitments.

4 NEW SECTION. **Sec. 8.** RESPONSIBILITIES OF CONTROLLERS. (1)  
5 *Transparency.*

6 (a) Controllers shall provide consumers with a reasonably  
7 accessible, clear, and meaningful privacy notice that includes:

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

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

11 (iii) How and where consumers may exercise the rights contained  
12 in section 6 of this act, including how a consumer may appeal a  
13 controller's action with regard to the consumer's request;

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

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

18 (b) If a controller sells personal data to third parties or  
19 processes personal data for targeted advertising, it must clearly and  
20 conspicuously disclose such processing, as well as the manner in  
21 which a consumer may exercise the right to opt out of such  
22 processing, in a clear and conspicuous manner.

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

27 (2) *Purpose specification.* A controller's collection of personal  
28 data must be limited to what is reasonably necessary in relation to  
29 the specified and express purposes for which such data are processed,  
30 as disclosed to the consumer.

31 (3) *Data minimization.* A controller's collection of personal data  
32 must be adequate, relevant, and limited to what is reasonably  
33 necessary in relation to the specified and express purposes for which  
34 such data are processed, as disclosed to the consumer.

35 (4) *Avoid secondary use.* Except as provided in this chapter, a  
36 controller may not process personal data for purposes that are not  
37 reasonably necessary to, or compatible with, the specified and  
38 express purposes for which such personal data are processed, as



1 disclosed to the consumer, unless the controller obtains the  
2 consumer's consent.

3 (5) *Security*. A controller shall establish, implement, and  
4 maintain reasonable administrative, technical, and physical data  
5 security practices to protect the confidentiality, integrity, and  
6 accessibility of personal data. Such data security practices shall be  
7 appropriate to the volume and nature of the personal data at issue.

8 (6) *Nondiscrimination*. A controller may not process personal data  
9 in violation of state and federal laws that prohibit unlawful  
10 discrimination against consumers. A controller shall not discriminate  
11 against a consumer for exercising any of the rights contained in this  
12 chapter, including denying goods or services to the consumer,  
13 charging different prices or rates for goods or services, and  
14 providing a different level of quality of goods and services to the  
15 consumer.

16 (7) *Sensitive data*. A controller may not process sensitive data  
17 concerning a consumer without obtaining the consumer's consent, or,  
18 in the case of the processing of personal data concerning a known  
19 child, without obtaining consent from the child's parent or lawful  
20 guardian.

21 (8) *Nonwaiver of consumer rights*. Any provision of a contract or  
22 agreement of any kind that purports to waive or limit in any way a  
23 consumer's rights under this chapter shall be deemed contrary to  
24 public policy and shall be void and unenforceable.

25 NEW SECTION. **Sec. 9.** DATA PROTECTION ASSESSMENTS. (1)  
26 Controllers must conduct, to the extent not previously conducted, a  
27 data protection assessment of each of their processing activities  
28 involving personal data and an additional data protection assessment  
29 any time there is a change in processing that materially increases  
30 the risk to consumers. Such data protection assessments must take  
31 into account the type of personal data to be processed by the  
32 controller, including the extent to which the personal data are  
33 sensitive data or otherwise sensitive in nature, and the context in  
34 which the personal data are to be processed.

35 (2) Data protection assessments conducted under subsection (1) of  
36 this section must identify and weigh the benefits that may flow  
37 directly and indirectly from the processing to the controller,  
38 consumer, other stakeholders, and the public against the potential  
39 risks to the rights of the consumer associated with such processing,

1 as mitigated by safeguards that can be employed by the controller to  
2 reduce such risks. The use of deidentified data and the reasonable  
3 expectations of consumers, as well as the context of the processing  
4 and the relationship between the controller and the consumer whose  
5 personal data will be processed, must be factored into this  
6 assessment by the controller.

7 (3) If the data protection assessment conducted under subsection  
8 (1) of this section determines that the potential risks of privacy  
9 harm to consumers are substantial and outweigh the interests of the  
10 controller, consumer, other stakeholders, and the public in  
11 processing the personal data of the consumer, the controller may only  
12 engage in such processing with the consent of the consumer or if  
13 another exemption under this chapter applies. To the extent the  
14 controller seeks consumer consent for processing, such consent must  
15 be as easy to withdraw as to give.

16 (4) Processing shall be presumed to be permissible unless: (a) It  
17 involves the processing of sensitive data; and (b) the risk of  
18 processing cannot be reduced by appropriate administrative and  
19 technical safeguards.

20 (5) The attorney general may request, in writing, that a  
21 controller disclose any data protection assessment that is relevant  
22 to an investigation conducted by the attorney general. The controller  
23 must make a data protection assessment available to the attorney  
24 general upon such a request. The attorney general may evaluate the  
25 data protection assessments for compliance with the duties contained  
26 in section 8 of this act and with other laws including, but not  
27 limited to, chapter 19.86 RCW. Data protection assessments are  
28 confidential and exempt from public inspection and copying under  
29 chapter 42.56 RCW. The disclosure of a data protection assessment  
30 pursuant to a request from the attorney general under this subsection  
31 does not constitute a waiver of the attorney-client privilege or work  
32 product protection with respect to the assessment and any information  
33 contained in the assessment.

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

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

1 (b) Comply with a civil, criminal, or regulatory inquiry,  
2 investigation, subpoena, or summons by federal, state, local, or  
3 other governmental authorities;

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

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

10 (e) Provide a product or service specifically requested by a  
11 consumer, perform a contract to which the consumer is a party, or  
12 take steps at the request of the consumer prior to entering into a  
13 contract;

14 (f) Protect the vital interests of the consumer or of another  
15 natural person;

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

21 (h) Process personal data for reasons of public interest in the  
22 areas of public health, or generalizable scientific, historical, or  
23 statistical research, but solely to the extent that the processing is  
24 (i) subject to suitable and specific measures to safeguard the rights  
25 of the consumer; and (ii) under the responsibility of a professional  
26 subject to confidentiality obligations under federal, state, or local  
27 law; or

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

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

33 (a) Conduct internal research to improve, repair, or develop  
34 products, services, or technology;

35 (b) Identify and repair technical errors that impair existing or  
36 intended functionality; or

37 (c) Perform internal operations that are reasonably aligned with  
38 the expectations of the consumer based on the consumer's existing  
39 relationship with the controller, or are otherwise compatible with  
40 processing in furtherance of the provision of a product or service

1 specifically requested by a consumer or the performance of a contract  
2 to which the consumer is a party.

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

10 (4) A controller or processor that discloses personal data to a  
11 third-party controller or processor in compliance with the  
12 requirements of this chapter is not in violation of this chapter if  
13 the recipient processes such personal data in violation of this  
14 chapter, provided that, at the time of disclosing the personal data,  
15 the disclosing controller or processor did not have actual knowledge  
16 that the recipient intended to commit a violation. A third-party  
17 controller or processor receiving personal data from a controller or  
18 processor in compliance with the requirements of this chapter is  
19 likewise not in violation of this chapter for the obligations of the  
20 controller or processor from which it receives such personal data.

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

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

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

28 (6) Personal data that are processed by a controller pursuant to  
29 this section must not be processed for any purpose other than those  
30 expressly listed in this section. Personal data that are processed by  
31 a controller pursuant to this section may be processed solely to the  
32 extent that such processing is: (i) Necessary, reasonable, and  
33 proportionate to the specific purpose or purposes listed in this  
34 section; and (ii) adequate, relevant, and limited to what is  
35 necessary in relation to the specific purpose or purposes listed in  
36 this section. Furthermore, personal data that are collected, used, or  
37 retained pursuant to subsection (2) of this section must, insofar as  
38 possible, taking into account the nature and purpose or purposes of  
39 such collection, use, or retention, be subjected to reasonable  
40 administrative, technical, and physical measures to protect the

1 confidentiality, integrity, and accessibility of the personal data,  
2 and to reduce reasonably foreseeable risks of harm to consumers  
3 relating to such collection, use, or retention of personal data.

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

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

12 NEW SECTION. **Sec. 11.** LIABILITY. (1) Any violation of this  
13 chapter shall not serve as the basis for, or be subject to, a private  
14 right of action under this chapter or under any other law. This does  
15 not relieve any party from any duties or obligations imposed, or to  
16 alter any independent rights that consumers have under other laws,  
17 chapter 19.86 RCW, the Washington state Constitution, or the United  
18 States Constitution.

19 (2) Where more than one controller or processor, or both a  
20 controller and a processor, involved in the same processing, is in  
21 violation of this chapter, the liability must be allocated among the  
22 parties according to principles of comparative fault, unless such  
23 liability is otherwise allocated by contract among the parties.

24 NEW SECTION. **Sec. 12.** ENFORCEMENT. (1) The attorney general has  
25 exclusive authority to enforce this chapter by bringing an action in  
26 the name of the state, or as *parens patriae* on behalf of persons  
27 residing in the state.

28 (2) Any controller or processor that violates this chapter is  
29 subject to an injunction and liable for a civil penalty of not more  
30 than seven thousand five hundred dollars for each violation.

31 NEW SECTION. **Sec. 13.** CONSUMER PRIVACY ACCOUNT. The consumer  
32 privacy account is created in the state treasury. All receipts from  
33 the imposition of civil penalties under this chapter must be  
34 deposited into the account except for the recovery of costs and  
35 attorneys' fees accrued by the attorney general in enforcing this  
36 chapter. Moneys in the account may be spent only after appropriation.  
37 Moneys in the account may only be used for the purposes of the office

1 of privacy and data protection as created under RCW 43.105.369, and  
2 may not be used to supplant general fund appropriations to the  
3 agency.

4 NEW SECTION. **Sec. 14.** PREEMPTION. This chapter supersedes and  
5 preempts laws, ordinances, regulations, or the equivalent adopted by  
6 any local entity regarding the processing of personal data by  
7 controllers or processors.

8 NEW SECTION. **Sec. 15.** PRIVACY OFFICE STUDY. (1) The state  
9 office of privacy and data protection shall conduct a study on the  
10 development of technology, such as a browser setting, browser  
11 extension, or global device setting, indicating a consumer's  
12 affirmative, freely given, and unambiguous choice to opt out of the  
13 processing of personal data for the purposes of targeted advertising,  
14 the sale of personal data, or profiling in furtherance of decisions  
15 that produce legal effects concerning consumers or similarly  
16 significant effects concerning consumers.

17 (2) The office of privacy and data protection shall submit a  
18 report of its findings and recommendations to the governor and the  
19 appropriate committees of the legislature by October 31, 2021.

20 NEW SECTION. **Sec. 16.** ATTORNEY GENERAL REPORT. (1) The attorney  
21 general shall compile a report evaluating the liability and  
22 enforcement provisions of this chapter including, but not limited to,  
23 the effectiveness of its efforts to enforce this chapter, and any  
24 recommendations for changes to such provisions.

25 (2) The attorney general shall submit the report to the governor  
26 and the appropriate committees of the legislature by July 1, 2022.

27 NEW SECTION. **Sec. 17.** JOINT RESEARCH INITIATIVES. The governor  
28 may enter into agreements with the governments of the Canadian  
29 province of British Columbia and the states of California and Oregon  
30 for the purpose of sharing personal data or personal information by  
31 public bodies across national and state borders to enable  
32 collaboration for joint data-driven research initiatives. Such  
33 agreements must provide reciprocal protections that the respective  
34 governments agree appropriately safeguard the data.

1        NEW SECTION.    **Sec. 18.**    FACIAL RECOGNITION. (1) Processors that  
2 provide facial recognition services must make available an  
3 application programming interface or other technical capability,  
4 chosen by the processor, to enable controllers or third parties to  
5 conduct legitimate, independent, and reasonable tests of those facial  
6 recognition services for accuracy and unfair performance differences  
7 across distinct subpopulations. Such subpopulations may be defined by  
8 race, skin tone, ethnicity, gender, age, disability status, or other  
9 protected characteristic that is objectively determinable or self-  
10 identified by the individuals portrayed in the testing dataset. If  
11 the results of that independent testing identify material unfair  
12 performance differences across subpopulations and those results are  
13 disclosed directly to the processor, who, acting reasonably,  
14 determines that the methodology and results of that testing are  
15 valid, then the processor must develop and implement a plan to  
16 address the identified performance differences. Nothing in this  
17 subsection prevents a processor from prohibiting the use of the  
18 processor's facial recognition service by a competitor for  
19 competitive purposes.

20        (2) Processors that provide facial recognition services must  
21 provide documentation that includes general information that:

22        (a) Explains the capabilities and limitations of the services in  
23 plain language; and

24        (b) Enables testing of the services in accordance with this  
25 section.

26        (3) Processors that provide facial recognition services must  
27 prohibit, in the contract required by section 5 of this act, the use  
28 of facial recognition services by controllers to unlawfully  
29 discriminate under federal or state law against individual consumers  
30 or groups of consumers.

31        (4) Controllers must provide a conspicuous and contextually  
32 appropriate notice whenever a facial recognition service is deployed  
33 in a physical premise open to the public that includes, at minimum,  
34 the following:

35        (a) The purpose or purposes for which the facial recognition  
36 service is deployed; and

37        (b) Information about where consumers can obtain additional  
38 information about the facial recognition service including, but not  
39 limited to, a link to any applicable online notice, terms, or policy  
40 that provides information about where and how consumers can exercise

1 any rights that they have with respect to the facial recognition  
2 service.

3 (5) Controllers must obtain consent from a consumer prior to  
4 enrolling an image of that consumer in a facial recognition service  
5 used in a physical premises open to the public.

6 (6) Except as provided in subsection (5) of this section,  
7 controllers may enroll an image of a consumer in a facial recognition  
8 service for a security or safety purpose without first obtaining  
9 consent from that consumer, provided that all of the following  
10 requirements are met:

11 (a) The controller must hold a reasonable suspicion, based on a  
12 specific incident, that the consumer has engaged in criminal  
13 activity, which includes, but is not limited to, shoplifting, fraud,  
14 stalking, or domestic violence;

15 (b) Any database used by a facial recognition service for  
16 identification, verification, or persistent tracking of consumers for  
17 a security or safety purpose must be used solely for that purpose and  
18 maintained separately from any other databases maintained by the  
19 controller;

20 (c) The controller must review any such database used by the  
21 controller's facial recognition service no less than biannually to  
22 remove facial templates of consumers whom the controller no longer  
23 holds a reasonable suspicion that they have engaged in criminal  
24 activity or that are more than three years old; and

25 (d) The controller must establish an internal process whereby a  
26 consumer may correct or challenge the decision to enroll the image of  
27 the consumer in a facial recognition service for a security or safety  
28 purpose.

29 (7) Controllers using a facial recognition service to make  
30 decisions that produce legal effects on consumers or similarly  
31 significant effects on consumers must ensure that those decisions are  
32 subject to meaningful human review.

33 (8) Prior to deploying a facial recognition service in the  
34 context in which it will be used, controllers must test the facial  
35 recognition service in operational conditions. Controllers must take  
36 commercially reasonable steps to ensure best quality results by  
37 following all reasonable guidance provided by the developer of the  
38 facial recognition service.

39 (9) Controllers using a facial recognition service must conduct  
40 periodic training of all individuals that operate a facial



1 recognition service or that process personal data obtained from the  
2 use of facial recognition services. Such training shall include, but  
3 not be limited to, coverage of:

4 (a) The capabilities and limitations of the facial recognition  
5 service;

6 (b) Procedures to interpret and act on the output of the facial  
7 recognition service; and

8 (c) The meaningful human review requirement for decisions that  
9 produce legal effects on consumers or similarly significant effects  
10 on consumers, to the extent applicable to the deployment context.

11 (10) Controllers shall not knowingly disclose personal data  
12 obtained from a facial recognition service to a law enforcement  
13 agency, except when such disclosure is:

14 (a) Pursuant to the consent of the consumer to whom the personal  
15 data relates;

16 (b) Required by federal, state, or local law in response to a  
17 court order, court-ordered warrant, or subpoena or summons issued by  
18 a judicial officer or grand jury;

19 (c) Necessary to prevent or respond to an emergency involving  
20 danger of death or serious physical injury to any person, upon a good  
21 faith belief by the controller; or

22 (d) To the national center for missing and exploited children, in  
23 connection with a report submitted thereto under Title 18 U.S.C. Sec.  
24 2258A.

25 (11) Controllers and processors that deploy a facial recognition  
26 service must respond to a consumer request to exercise the rights  
27 specified in section 6 of this act and must fulfill the duties  
28 identified in section 8 of this act.

29 NEW SECTION. **Sec. 19.** Sections 1 through 18 and 20 of this act  
30 constitute a new chapter in Title 19 RCW.

31 NEW SECTION. **Sec. 20.** Except for section 15 of this act, this  
32 act takes effect July 31, 2021.

--- END ---