

---

**SUBSTITUTE SENATE BILL 5062**

---

**State of Washington**

**67th Legislature**

**2021 Regular Session**

**By** Senate Environment, Energy & Technology (originally sponsored by Senators Carlyle, Nguyen, Billig, Darneille, Das, Dhingra, Holy, Hunt, Lovelett, Mullet, Pedersen, Salomon, Sheldon, Wellman, and Wilson, C.)

READ FIRST TIME 01/22/21.

1 AN ACT Relating to the management, oversight, and use of data;  
2 adding a new section to chapter 42.56 RCW; adding new chapters to  
3 Title 19 RCW; adding a new chapter to Title 43 RCW; creating new  
4 sections; prescribing penalties; providing an effective date;  
5 providing an expiration date; and declaring an emergency.

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

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

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

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

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

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

21 (4) Responding to COVID-19 illustrates the need for public  
22 policies that protect individual privacy while fostering  
23 technological innovation. For years, contact tracing best practices  
24 have been used by public health officials to securely process high  
25 value individual data and have effectively stopped the prolific  
26 spread of infectious diseases. However, the scale of COVID-19 is  
27 unprecedented. Contact tracing is evolving in a manner that  
28 necessitates the use of technology to rapidly collect and process  
29 data from multiple data sets, many of which are unanticipated, to  
30 protect public health as well as to facilitate the continued safe  
31 operation of the economy. The benefits of such technology, however,  
32 should not supersede the potential privacy risks to individuals.

33 (5) Exposure notification applications have already been deployed  
34 throughout the country and the world. However, contact tracing  
35 technology is rapidly evolving. Applications may be integrated in a  
36 manner that facilitates the aggregation and sharing of individual  
37 data that in effect generate profiles of individuals. Artificial  
38 intelligence may be used for the extrapolation of data to analyze and  
39 interpret data for public health purposes. Moreover, the potential  
40 government use of exposure notification applications poses additional

1 potential privacy risks to individuals due to the types of sensitive  
2 data it has access to and processes. Much of that processing may have  
3 legal effects, including access to services or establishments. The  
4 capabilities of next generation contact tracing technologies are  
5 unknown and policies must be in place to provide privacy protections  
6 for current uses as well as potential future uses.

7 (6) With this act, the legislature intends to: Provide a modern  
8 privacy regulatory framework with data privacy guardrails to protect  
9 individual privacy; instill public confidence on the processing of  
10 their personal and public health data during any global pandemic; and  
11 require companies to be responsible custodians of data as  
12 technological innovations emerge.

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

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

30 (9) Lastly, the legislature encourages the state office of  
31 privacy and data protection to monitor (1) the development of  
32 universal privacy controls that communicate a consumer's affirmative,  
33 freely given, and unambiguous choice to opt out of the processing of  
34 their personal data, and (2) the effectiveness of allowing a consumer  
35 to designate a third party to exercise a consumer right on their  
36 behalf as authorized in other privacy laws.

37 **PART 1**

38 **Personal Data Privacy Regulations—Private Sector**

1        NEW SECTION.        **Sec. 101.**        DEFINITIONS. The definitions in this  
2 section apply throughout this chapter unless the context clearly  
3 requires otherwise.

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

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

15        (3) "Authenticate" means to use reasonable means to determine  
16 that a request to exercise any of the rights in section 103 (1)  
17 through (4) of this act is being made by the consumer who is entitled  
18 to exercise such rights with respect to the personal data at issue.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 (20) "Legislative agencies" has the same meaning as defined in  
2 RCW 44.80.020.

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

4 (22) "Nonprofit corporation" has the same meaning as in RCW  
5 24.03.005.

6 (23)(a) "Personal data" means any information that is linked or  
7 reasonably linkable to an identified or identifiable natural person.  
8 "Personal data" does not include deidentified data or publicly  
9 available information.

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

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

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

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

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

28 (28) "Pseudonymous data" means personal data that cannot be  
29 attributed to a specific natural person without the use of additional  
30 information, provided that such additional information is kept  
31 separately and is subject to appropriate technical and organizational  
32 measures to ensure that the personal data are not attributed to an  
33 identified or identifiable natural person.

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

37 (b) "Sale" does not include the following: (i) The disclosure of  
38 personal data to a processor who processes the personal data on  
39 behalf of the controller; (ii) the disclosure of personal data to a  
40 third party with whom the consumer has a direct relationship for

1 purposes of providing a product or service requested by the consumer;  
2 (iii) the disclosure or transfer of personal data to an affiliate of  
3 the controller; (iv) the disclosure of information that the consumer  
4 (A) intentionally made available to the general public via a channel  
5 of mass media, and (B) did not restrict to a specific audience; or  
6 (v) the disclosure or transfer of personal data to a third party as  
7 an asset that is part of a merger, acquisition, bankruptcy, or other  
8 transaction in which the third party assumes control of all or part  
9 of the controller's assets.

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

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

24 (32) "State agency" has the same meaning as in RCW 43.105.020.

25 (33) "Targeted advertising" means displaying advertisements to a  
26 consumer where the advertisement is selected based on personal data  
27 obtained from a consumer's activities over time and across  
28 nonaffiliated websites or online applications to predict the  
29 consumer's preferences or interests. It does not include advertising:  
30 (a) Based on activities within a controller's own websites or online  
31 applications; (b) based on the context of a consumer's current search  
32 query or visit to a website or online application; or (c) to a  
33 consumer in response to the consumer's request for information or  
34 feedback.

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

38 NEW SECTION. **Sec. 102.** JURISDICTIONAL SCOPE. (1) This chapter  
39 applies to legal entities that conduct business in Washington or

1 produce products or services that are targeted to residents of  
2 Washington, and that satisfy one or more of the following thresholds:

3 (a) During a calendar year, controls or processes personal data  
4 of 100,000 consumers or more; or

5 (b) Derives over 25 percent of gross revenue from the sale of  
6 personal data and processes or controls personal data of 25,000  
7 consumers or more.

8 (2) This chapter does not apply to:

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

11 (b) Municipal corporations;

12 (c) Air carriers;

13 (d) Information that meets the definition of:

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

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

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

20 (iv) Identifiable private information for purposes of the federal  
21 policy for the protection of human subjects, 45 C.F.R. Part 46;  
22 identifiable private information that is otherwise information  
23 collected as part of human subjects research pursuant to the good  
24 clinical practice guidelines issued by the international council for  
25 harmonization; the protection of human subjects under 21 C.F.R. Parts  
26 50 and 56; or personal data used or shared in research conducted in  
27 accordance with one or more of the requirements set forth in this  
28 subsection;

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

31 (A) A quality improvement committee for purposes of RCW  
32 43.70.510, 70.230.080, or 70.41.200;

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

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

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

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

4 (vii) Patient safety work product for purposes of 42 C.F.R. Part  
5 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26; or

6 (viii) Information that is (A) deidentified in accordance with  
7 the requirements for deidentification set forth in 45 C.F.R. Part  
8 164, and (B) derived from any of the health care-related information  
9 listed in this subsection (2)(d);

10 (e) Information originating from, and intermingled to be  
11 indistinguishable with, information under (d) of this subsection that  
12 is maintained by:

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

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

18 (iii) A program or a qualified service organization as defined by  
19 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

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

22 (g)(i) An activity involving the collection, maintenance,  
23 disclosure, sale, communication, or use of any personal information  
24 bearing on a consumer's credit worthiness, credit standing, credit  
25 capacity, character, general reputation, personal characteristics, or  
26 mode of living by a consumer reporting agency, as defined in Title 15  
27 U.S.C. Sec. 1681a(f), by a furnisher of information, as set forth in  
28 Title 15 U.S.C. Sec. 1681s-2, who provides information for use in a  
29 consumer report, as defined in Title 15 U.S.C. Sec. 1681a(d), and by  
30 a user of a consumer report, as set forth in Title 15 U.S.C. Sec.  
31 1681b.

32 (ii) (e)(i) of this subsection applies only to the extent that  
33 such an activity involving the collection, maintenance, disclosure,  
34 sale, communication, or use of such information by that agency,  
35 furnisher, or user is subject to regulation under the fair credit  
36 reporting act, Title 15 U.S.C. Sec. 1681 et seq., and the information  
37 is not collected, maintained, used, communicated, disclosed, or sold  
38 except as authorized by the fair credit reporting act;

39 (h) Personal data collected and maintained for purposes of  
40 chapter 43.71 RCW;

1 (i) Personal data collected, processed, sold, or disclosed  
2 pursuant to the federal Gramm-Leach-Bliley act (P.L. 106-102), and  
3 implementing regulations, if the collection, processing, sale, or  
4 disclosure is in compliance with that law;

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

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

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

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

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

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

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

36 NEW SECTION. **Sec. 103.** CONSUMER RIGHTS. (1) A consumer has the  
37 right to confirm whether or not a controller is processing personal  
38 data concerning the consumer and access the categories of personal  
39 data the controller is processing.

1 (2) A consumer has the right to correct inaccurate personal data  
2 concerning the consumer, taking into account the nature of the  
3 personal data and the purposes of the processing of the personal  
4 data.

5 (3) A consumer has the right to delete personal data concerning  
6 the consumer.

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

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

18 NEW SECTION. **Sec. 104.** EXERCISING CONSUMER RIGHTS. (1)

19 Consumers may exercise the rights set forth in section 103 of this  
20 act by submitting a request, at any time, to a controller specifying  
21 which rights the individual wishes to exercise.

22 (2) In the case of processing personal data concerning a known  
23 child, the parent or legal guardian of the known child may exercise  
24 the rights of this chapter on the child's behalf.

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

30 NEW SECTION. **Sec. 105.** RESPONDING TO REQUESTS. (1) Except as

31 provided in this chapter, the controller must comply with a request  
32 to exercise the rights pursuant to section 103 of this act.

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

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

5 (3) A controller must comply with a request to exercise the right  
6 in section 103(5) of this act as soon as feasibly possible, but no  
7 later than 15 days of receipt of the request.

8 (4)(a) A controller must inform a consumer of any action taken on  
9 a request to exercise any of the rights in section 103 (2) through  
10 (4) of this act without undue delay and in any event within 45 days  
11 of receipt of the request. That period may be extended once by 45  
12 additional days where reasonably necessary, taking into account the  
13 complexity and number of the requests. The controller must inform the  
14 consumer of any such extension within 45 days of receipt of the  
15 request, together with the reasons for the delay.

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

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

30 (d) A controller is not required to comply with a request to  
31 exercise any of the rights under section 103 (1) through (4) of this  
32 act if the controller is unable to authenticate the request using  
33 commercially reasonable efforts. In such a case, the controller may  
34 request the provision of additional information reasonably necessary  
35 to authenticate the request.

36 (5)(a) Controllers must establish an internal process whereby  
37 consumers may appeal a refusal to take action on a request to  
38 exercise any of the rights under section 103 of this act within a  
39 reasonable period of time after the consumer's receipt of the notice  
40 sent by the controller under subsection (4)(b) of this section.

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

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

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

26 NEW SECTION. **Sec. 106.** RESPONSIBILITY ACCORDING TO ROLE. (1)  
27 Controllers and processors are responsible for meeting their  
28 respective obligations established under this chapter.

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

33 (a) Taking into account the nature of the processing, the  
34 processor shall assist the controller by appropriate technical and  
35 organizational measures, insofar as this is possible, for the  
36 fulfillment of the controller's obligation to respond to consumer  
37 requests to exercise their rights pursuant to section 103 of this  
38 act; and

1 (b) Taking into account the nature of processing and the  
2 information available to the processor, the processor shall: Assist  
3 the controller in meeting the controller's obligations in relation to  
4 the security of processing the personal data and in relation to the  
5 notification of a breach of the security of the system pursuant to  
6 RCW 19.255.010; and provide information to the controller necessary  
7 to enable the controller to conduct and document any data protection  
8 assessments required by section 109 of this act. The controller and  
9 processor are each responsible for only the measures allocated to  
10 them.

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

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

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

20 (4) Taking into account the context of processing, the controller  
21 and the processor shall implement appropriate technical and  
22 organizational measures to ensure a level of security appropriate to  
23 the risk and establish a clear allocation of the responsibilities  
24 between them to implement such measures.

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

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

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

1 (ii) The processor shall allow for, and contribute to, reasonable  
2 audits and inspections by the controller or the controller's  
3 designated auditor. Alternatively, the processor may, with the  
4 controller's consent, arrange for a qualified and independent auditor  
5 to conduct, at least annually and at the processor's expense, an  
6 audit of the processor's policies and technical and organizational  
7 measures in support of the obligations under this chapter using an  
8 appropriate and accepted control standard or framework and audit  
9 procedure for the audits as applicable, and provide a report of the  
10 audit to the controller upon request.

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

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

26 NEW SECTION. **Sec. 107.** RESPONSIBILITIES OF CONTROLLERS. (1) (a)  
27 Controllers shall provide consumers with a reasonably accessible,  
28 clear, and meaningful privacy notice that includes:

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

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

32 (iii) How and where consumers may exercise the rights contained  
33 in section 103 of this act, including how a consumer may appeal a  
34 controller's action with regard to the consumer's request;

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

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

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

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

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

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

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

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

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

1 controller as part of such a program unless: (a) The sale is  
2 reasonably necessary to enable the third party to provide a benefit  
3 to which the consumer is entitled; (b) the sale of personal data to  
4 third parties is clearly disclosed in the terms of the program; and  
5 (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) 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 concerning a known child, without obtaining consent  
13 from the child's parent or lawful guardian, in accordance with the  
14 children's online privacy protection act requirements.

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

19 NEW SECTION. **Sec. 108.** PROCESSING DEIDENTIFIED DATA OR  
20 PSEUDONYMOUS DATA. (1) This chapter does not require a controller or  
21 processor to do any of the following solely for purposes of complying  
22 with this chapter:

23 (a) Reidentify deidentified data;

24 (b) Comply with an authenticated consumer request to access,  
25 correct, delete, or port personal data pursuant to section 103 (1)  
26 through (4) of this act, if all of the following are true:

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

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

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

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

4 (2) The rights contained in section 103 (1) through (4) of this  
5 act do not apply to pseudonymous data in cases where the controller  
6 is able to demonstrate any information necessary to identify the  
7 consumer is kept separately and is subject to effective technical and  
8 organizational controls that prevent the controller from accessing  
9 such information.

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

15 NEW SECTION. **Sec. 109.** DATA PROTECTION ASSESSMENTS. (1)

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

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

20 (b) The processing of personal data for the purposes of the sale  
21 of personal data;

22 (c) The processing of personal data for purposes of profiling,  
23 where such profiling presents a reasonably foreseeable risk of: (i)  
24 Unfair or deceptive treatment of, or disparate impact on, consumers;  
25 (ii) financial, physical, or reputational injury to consumers; (iii)  
26 a physical or other intrusion upon the solitude or seclusion, or the  
27 private affairs or concerns, of consumers, where such intrusion would  
28 be offensive to a reasonable person; or (iv) other substantial injury  
29 to consumers;

30 (d) The processing of sensitive data; and

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

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

37 (2) Data protection assessments conducted under subsection (1) of  
38 this section must identify and weigh the benefits that may flow  
39 directly and indirectly from the processing to the controller,

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

9 (3) The attorney general may request, in writing, that a  
10 controller disclose any data protection assessment that is relevant  
11 to an investigation conducted by the attorney general. The controller  
12 must make a data protection assessment available to the attorney  
13 general upon such a request. The attorney general may evaluate the  
14 data protection assessments for compliance with the responsibilities  
15 contained in section 107 of this act and, if it serves a civil  
16 investigative demand, with RCW 19.86.110. Data protection assessments  
17 are confidential and exempt from public inspection and copying under  
18 chapter 42.56 RCW. The disclosure of a data protection assessment  
19 pursuant to a request from the attorney general under this subsection  
20 does not constitute a waiver of the attorney-client privilege or work  
21 product protection with respect to the assessment and any information  
22 contained in the assessment unless otherwise subject to case law  
23 regarding the applicability of attorney-client privilege or work  
24 product protections.

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

28 NEW SECTION. **Sec. 110.** LIMITATIONS AND APPLICABILITY. (1) The  
29 obligations imposed on controllers or processors under this chapter  
30 do not restrict a controller's or processor's ability to:

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

33 (b) Comply with a civil, criminal, or regulatory inquiry,  
34 investigation, subpoena, or summons by federal, state, local, or  
35 other governmental authorities;

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

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

3 (e) Provide a product or service specifically requested by a  
4 consumer, perform a contract to which the consumer is a party, or  
5 take steps at the request of the consumer prior to entering into a  
6 contract;

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

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

15 (h) Engage in public or peer-reviewed scientific, historical, or  
16 statistical research in the public interest that adheres to all other  
17 applicable ethics and privacy laws and is approved, monitored, and  
18 governed by an institutional review board, human subjects research  
19 ethics review board, or a similar independent oversight entity that  
20 determines: (i) If the research is likely to provide substantial  
21 benefits that do not exclusively accrue to the controller; (ii) the  
22 expected benefits of the research outweigh the privacy risks; and  
23 (iii) if the controller has implemented reasonable safeguards to  
24 mitigate privacy risks associated with research, including any risks  
25 associated with reidentification; or

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

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

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

33 (b) Perform solely internal operations that are reasonably  
34 aligned with the expectations of the consumer based on the consumer's  
35 existing relationship with the controller, or are otherwise  
36 compatible with processing in furtherance of the provision of a  
37 product or service specifically requested by a consumer or the  
38 performance of a contract to which the consumer is a party when those  
39 internal operations are performed during, and not following, the  
40 consumer's relationship with the controller.

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

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

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

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

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

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

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

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

37 (b) Personal data that is processed by a controller pursuant to  
38 this section may be processed solely to the extent that such  
39 processing is: (i) Necessary, reasonable, and proportionate to the  
40 purposes listed in this section; (ii) adequate, relevant, and limited

1 to what is necessary in relation to the specific purpose or purposes  
2 listed in this section; and (iii) insofar as possible, taking into  
3 account the nature and purpose of processing the personal data,  
4 subjected to reasonable administrative, technical, and physical  
5 measures to protect the confidentiality, integrity, and accessibility  
6 of the personal data, and to reduce reasonably foreseeable risks of  
7 harm to consumers.

8 NEW SECTION. **Sec. 111.** PRIVATE RIGHT OF ACTION. (1) A violation  
9 of this chapter may not serve as the basis for, or be subject to, a  
10 private right of action under this chapter or under any other law.

11 (2) Rights possessed by consumers as of July 1, 2020, under  
12 chapter 19.86 RCW, the Washington state Constitution, the United  
13 States Constitution, or other laws are not altered.

14 NEW SECTION. **Sec. 112.** ENFORCEMENT. (1) This chapter may be  
15 enforced solely by the attorney general under the consumer protection  
16 act, chapter 19.86 RCW.

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

25 (3) The legislative declarations in this section shall not apply  
26 to any claim or action by any party other than the attorney general  
27 alleging that conduct regulated by this chapter violates chapter  
28 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

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

1 (5) A controller or processor found in violation of this chapter  
2 is subject to a civil penalty of up to \$7,500 for each violation.

3 (6) In any action brought under this section, the state is  
4 entitled to recover, in addition to the penalties prescribed in  
5 subsection (5) of this section, the costs of investigation, including  
6 reasonable attorneys' fees.

7 (7) All receipts from the imposition of civil penalties under  
8 this chapter must be deposited into the consumer privacy account  
9 created in section 113 of this act.

10 NEW SECTION. **Sec. 113.** CONSUMER PRIVACY ACCOUNT. The consumer  
11 privacy account is created in the state treasury. All receipts from  
12 the imposition of civil penalties under this chapter must be  
13 deposited into the account. Moneys in the account may be spent only  
14 after appropriation. Moneys in the account may only be used for the  
15 purposes of recovery of costs and attorneys' fees accrued by the  
16 attorney general in enforcing this chapter and for the office of  
17 privacy and data protection as created in RCW 43.105.369. Moneys may  
18 not be used to supplant general fund appropriations to either agency.

19 NEW SECTION. **Sec. 114.** PREEMPTION. (1) Except as provided in  
20 this section, this chapter supersedes and preempts laws, ordinances,  
21 regulations, or the equivalent adopted by any local entity regarding  
22 the processing of personal data by controllers or processors.

23 (2) Laws, ordinances, or regulations regarding the processing of  
24 personal data by controllers or processors that are adopted by any  
25 local entity prior to July 1, 2020, are not superseded or preempted.

26 NEW SECTION. **Sec. 115.** If any provision of this act or its  
27 application to any person or circumstance is held invalid, the  
28 remainder of the act or the application of the provision to other  
29 persons or circumstances is not affected.

30 NEW SECTION. **Sec. 116.** PRIVACY OFFICE REPORT. (1) The state  
31 office of privacy and data protection, in collaboration with the  
32 office of the attorney general, shall research and examine existing  
33 analysis on the development of technology, such as a browser setting,  
34 browser extension, or global device setting, indicating a consumer's  
35 affirmative, freely given, and unambiguous choice to opt out of the  
36 processing of personal data for the purposes of targeted advertising,

1 the sale of personal data, or profiling in furtherance of decisions  
2 that produce legal effects concerning consumers or similarly  
3 significant effects concerning consumers. A contracted study is not  
4 required.

5 (2) The office of privacy and data protection shall submit a  
6 report of its findings and will identify specific recommendations to  
7 the governor and the appropriate committees of the legislature by  
8 December 1, 2022.

9 NEW SECTION. **Sec. 117.** A new section is added to chapter 42.56  
10 RCW to read as follows:

11 Data protection assessments submitted by a controller to the  
12 attorney general in accordance with requirements under section 109 of  
13 this act are exempt from disclosure under this chapter.

## 14 **PART 2**

### 15 **Data Privacy Regarding Public Health Emergency—Private Sector**

16 NEW SECTION. **Sec. 201.** The definitions in this section apply  
17 throughout this chapter unless the context clearly requires  
18 otherwise.

19 (1) "Authenticate" means to use reasonable means to determine  
20 that a request to exercise any of the rights in section 203 of this  
21 act is being made by the consumer who is entitled to exercise the  
22 rights with respect to the covered data at issue.

23 (2) "Business associate" has the same meaning as in Title 45  
24 C.F.R. Part 160, established pursuant to the federal health insurance  
25 portability and accountability act of 1996.

26 (3) "Child" has the same meaning as defined in the children's  
27 online privacy protection act, Title 15 U.S.C. Sec. 6501 through  
28 6506.

29 (4) "Consent" means a clear affirmative act signifying a freely  
30 given, specific, informed, and unambiguous indication of a consumer's  
31 agreement to the processing of covered data relating to the consumer,  
32 such as by a written statement, including by electronic means, or  
33 other clear affirmative action.

34 (5) (a) "Consumer" means a natural person who is a Washington  
35 resident acting only in an individual or household context.

36 (b) "Consumer" does not include a natural person acting in a  
37 commercial or employment context.

1 (6) "Controller" means the natural or legal person that, alone or  
2 jointly with others, determines the purposes and means of the  
3 processing of covered data.

4 (7) "Covered data" includes personal data and one or more of the  
5 following: Specific geolocation data; proximity data; or personal  
6 health data.

7 (8) "Covered entity" has the same meaning as defined in Title 45  
8 C.F.R. Part 160, established pursuant to the federal health insurance  
9 portability and accountability act of 1996.

10 (9) "Covered purpose" means processing of covered data concerning  
11 a consumer for the purposes of detecting symptoms of an infectious  
12 disease, enabling the tracking of a consumer's contacts with other  
13 consumers, or with specific locations to identify in an automated  
14 fashion whom consumers have come into contact with, or digitally  
15 notifying, in an automated manner, a consumer who may have become  
16 exposed to an infectious disease, or other similar purposes directly  
17 related to a state of emergency declared by the governor pursuant to  
18 RCW 43.06.010 and any restrictions imposed under the state of  
19 emergency declared by the governor pursuant to RCW 43.06.200 through  
20 43.06.270.

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

30 (11) "Delete" means to remove or destroy information such that it  
31 is not maintained in human or machine-readable form and cannot be  
32 retrieved or utilized in the course of business.

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

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

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

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

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

4 (17)(a) "Personal data" means any information that is linked or  
5 reasonably linkable to an identified or identifiable natural person.

6 "Personal data" does not include deidentified data or publicly  
7 available information.

8 (b) For the purposes of this subsection, "publicly available  
9 information" means information that is lawfully made available from  
10 federal, state, or local government records.

11 (18) "Personal health data" means information relating to the  
12 past, present, or future diagnosis or treatment of a consumer  
13 regarding an infectious disease.

14 (19) "Process," "processed," or "processing" means any operation  
15 or set of operations that are performed on covered data or on sets of  
16 covered data by automated means, such as the collection, use,  
17 storage, disclosure, analysis, deletion, or modification of covered  
18 data.

19 (20) "Processor" means a natural or legal person that processes  
20 covered data on behalf of a controller.

21 (21) "Protected health information" has the same meaning as  
22 defined in Title 45 C.F.R. Sec. 160.103, established pursuant to the  
23 federal health insurance portability and accountability act of 1996.

24 (22) "Proximity data" means technologically derived information  
25 that identifies past or present proximity of one consumer to another,  
26 or the proximity of natural persons to other locations or objects.

27 (23) "Secure" means encrypted in a manner that meets or exceeds  
28 the national institute of standards and technology standard or is  
29 otherwise modified so that the covered data is rendered unreadable,  
30 unusable, or undecipherable by an unauthorized person.

31 (24) "Sell" means the exchange of covered data for monetary or  
32 other valuable consideration by the controller to a third party.

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

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

4 NEW SECTION. **Sec. 202.** PROHIBITIONS. Except as provided in this  
5 chapter, it is unlawful for a controller or processor to:

6 (1) Process covered data for a covered purpose unless:

7 (a) The controller or processor provides the consumer with a  
8 privacy notice as required in section 207 of this act prior to or at  
9 the time of the processing; and

10 (b) The consumer provides consent for the processing;

11 (2) Disclose any covered data processed for a covered purpose to  
12 federal, state, or local law enforcement;

13 (3) Sell any covered data processed for a covered purpose; or

14 (4) Share any covered data processed for a covered purpose with  
15 another controller, processor, or third party unless the sharing is  
16 governed by contract pursuant to section 206 of this act and is  
17 disclosed to a consumer in the notice required in section 207 of this  
18 act.

19 NEW SECTION. **Sec. 203.** CONSUMER RIGHTS. (1) A consumer has the  
20 right to opt out of the processing of covered data concerning the  
21 consumer for a covered purpose.

22 (2) A consumer has the right to confirm whether or not a  
23 controller is processing covered data concerning the consumer for a  
24 covered purpose and access the covered data.

25 (3) A consumer has the right to request correction of inaccurate  
26 covered data concerning the consumer processed for a covered purpose.

27 (4) A consumer has the right to request deletion of covered data  
28 concerning the consumer processed for a covered purpose.

29 NEW SECTION. **Sec. 204.** EXERCISING CONSUMER RIGHTS. (1)  
30 Consumers may exercise their rights set forth in section 203 of this  
31 act by submitting a request, at any time, to a controller specifying  
32 which rights the individual wishes to exercise.

33 (2) In the case of processing personal data concerning a known  
34 child, the parent or legal guardian of the known child may exercise  
35 the rights of this chapter on the child's behalf.

36 (3) In the case of processing personal data concerning a consumer  
37 subject to guardianship, conservatorship, or other protective

1 arrangement under chapter 11.88, 11.92, or 11.130 RCW, the guardian  
2 or the conservator of the consumer may exercise the rights of this  
3 chapter on the consumer's behalf.

4 NEW SECTION. **Sec. 205.** RESPONDING TO REQUESTS. (1) Except as  
5 provided in this chapter, controllers that process covered data for a  
6 covered purpose must comply with a request to exercise the rights  
7 pursuant to section 203 of this act.

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

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

17 (3) A controller must comply with a request to exercise the right  
18 in section 203(1) of this act as soon as feasibly possible, but no  
19 later than 15 days of receipt of the request.

20 (4) (a) A controller must inform a consumer of any action taken on  
21 a request to exercise any of the rights in section 203 (2) through  
22 (4) of this act without undue delay and in any event within 45 days  
23 of receipt of the request. That period may be extended once by 45  
24 additional days where reasonably necessary, taking into account the  
25 complexity and number of the requests. The controller must inform the  
26 consumer of any such extension within 45 days of receipt of the  
27 request, together with the reasons for the delay.

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

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

1 controller bears the burden of demonstrating the manifestly unfounded  
2 or excessive character of the request.

3 (d) A controller is not required to comply with a request to  
4 exercise any of the rights under section 203 (1) through (4) of this  
5 act if the controller is unable to authenticate the request using  
6 commercially reasonable efforts. In such a case, the controller may  
7 request the provision of additional information reasonably necessary  
8 to authenticate the request.

9 (5)(a) Controllers must establish an internal process whereby  
10 consumers may appeal a refusal to take action on a request to  
11 exercise any of the rights under section 203 of this act within a  
12 reasonable period of time after the consumer's receipt of the notice  
13 sent by the controller under subsection (4)(b) of this section.

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

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

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

1        NEW SECTION.    **Sec. 206.**    RESPONSIBILITY ACCORDING TO ROLE. (1)

2    Controllers and processors are responsible for meeting their  
3    respective obligations established under this chapter.

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

8        (a) Taking into account the nature of the processing, the  
9    processor shall assist the controller by appropriate technical and  
10   organizational measures, insofar as this is possible, for the  
11   fulfillment of the controller's obligation to respond to consumer  
12   requests to exercise their rights pursuant to section 203 of this  
13   act; and

14       (b) Taking into account the nature of processing and the  
15   information available to the processor, the processor shall assist  
16   the controller in meeting the controller's obligations in relation to  
17   the security of processing the personal data and in relation to the  
18   notification of a breach of the security of the system pursuant to  
19   RCW 19.255.010.

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

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

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

29       (4) Taking into account the context of processing, the controller  
30   and the processor shall implement appropriate technical and  
31   organizational measures to ensure a level of security appropriate to  
32   the risk and establish a clear allocation of the responsibilities  
33   between them to implement such measures.

34       (5) Processing by a processor must be governed by a contract  
35   between the controller and the processor that is binding on both  
36   parties and that sets out the processing instructions to which the  
37   processor is bound, including the nature and purpose of the  
38   processing, the type of personal data subject to the processing, the  
39   duration of the processing, and the obligations and rights of both  
40   parties. In addition, the contract must include the requirements

1 imposed by this subsection and subsections (3) and (4) of this  
2 section, as well as the following requirements:

3 (a) At the choice of the controller, the processor shall delete  
4 or return all personal data to the controller as requested at the end  
5 of the provision of services, unless retention of the personal data  
6 is required by law;

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

10 (ii) The processor shall allow for, and contribute to, reasonable  
11 audits and inspections by the controller or the controller's  
12 designated auditor. Alternatively, the processor may, with the  
13 controller's consent, arrange for a qualified and independent auditor  
14 to conduct, at least annually and at the processor's expense, an  
15 audit of the processor's policies and technical and organizational  
16 measures in support of the obligations under this chapter using an  
17 appropriate and accepted control standard or framework and audit  
18 procedure for the audits as applicable, and provide a report of the  
19 audit to the controller upon request.

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

23 (7) Determining whether a person is acting as a controller or  
24 processor with respect to a specific processing of data is a fact-  
25 based determination that depends upon the context in which personal  
26 data is to be processed. A person that is not limited in its  
27 processing of personal data pursuant to a controller's instructions,  
28 or that fails to adhere to such instructions, is a controller and not  
29 a processor with respect to a specific processing of data. A  
30 processor that continues to adhere to a controller's instructions  
31 with respect to a specific processing of personal data remains a  
32 processor. If a processor begins, alone or jointly with others,  
33 determining the purposes and means of the processing of personal  
34 data, it is a controller with respect to the processing.

35 NEW SECTION. **Sec. 207.** RESPONSIBILITIES OF CONTROLLERS. (1)  
36 Controllers that process covered data for a covered purpose must  
37 provide consumers with a clear and conspicuous privacy notice that  
38 includes, at a minimum:

1 (a) How a consumer may exercise the rights contained in section  
2 203 of this act, including how a consumer may appeal a controller's  
3 action with regard to the consumer's request;

4 (b) The categories of covered data processed by the controller;

5 (c) The purposes for which the categories of covered data are  
6 processed;

7 (d) The categories of covered data that the controller shares  
8 with third parties, if any; and

9 (e) The categories of third parties, if any, with whom the  
10 controller shares covered data.

11 (2) A controller's collection of covered data must be limited to  
12 what is reasonably necessary in relation to the covered purposes for  
13 which the data is processed.

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

17 (4) Except as provided in this chapter, a controller may not  
18 process covered data for purposes that are not reasonably necessary  
19 to, or compatible with, the covered purposes for which the personal  
20 data is processed unless the controller obtains the consumer's  
21 consent. Controllers may not process covered data or deidentified  
22 data that was processed for a covered purpose for purposes of  
23 marketing, developing new products or services, or engaging in  
24 commercial product or market research.

25 (5) A controller shall establish, implement, and maintain  
26 reasonable administrative, technical, and physical data security  
27 practices to protect the confidentiality, integrity, and  
28 accessibility of covered data. The data security practices must be  
29 appropriate to the volume and nature of the personal data at issue.

30 (6) A controller must delete or deidentify all covered data  
31 processed for a covered purpose when the data is no longer being used  
32 for the covered purpose.

33 (7) A controller may not process personal data on the basis of a  
34 consumer's or a class of consumers' actual or perceived race, color,  
35 ethnicity, religion, national origin, sex, gender, gender identity,  
36 sexual orientation, familial status, lawful source of income, or  
37 disability, in a manner that unlawfully discriminates against the  
38 consumer or class of consumers with respect to the offering or  
39 provision of: (a) Housing; (b) employment; (c) credit; (d) education;

1 or (e) the goods, services, facilities, privileges, advantages, or  
2 accommodations of any place of public accommodation.

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

7 NEW SECTION. **Sec. 208.** LIMITATIONS AND APPLICABILITY. (1) The  
8 obligations imposed on controllers or processors under this chapter  
9 do not restrict a controller's or processor's ability to:

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

12 (b) Process deidentified information to engage in public or peer-  
13 reviewed scientific, historical, or statistical research in the  
14 public interest that adheres to all other applicable ethics and  
15 privacy laws and is approved, monitored, and governed by an  
16 institutional review board, human subjects research ethics review  
17 board, or a similar independent oversight entity that determines: (i)  
18 If the research is likely to provide substantial benefits that do not  
19 exclusively accrue to the controller; (ii) the expected benefits of  
20 the research outweigh the privacy risks; and (iii) if the controller  
21 has implemented reasonable safeguards to mitigate privacy risks  
22 associated with research, including any risks associated with  
23 reidentification.

24 (2) This chapter does not apply to:

25 (a) Information that meets the definition of:

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

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

31 (iii) Identifiable private information for purposes of the  
32 federal policy for the protection of human subjects, 45 C.F.R. Part  
33 46; identifiable private information that is otherwise information  
34 collected as part of human subjects research pursuant to the good  
35 clinical practice guidelines issued by the international council for  
36 harmonization; the protection of human subjects under 21 C.F.R. Parts  
37 50 and 56; or personal data used or shared in research conducted in  
38 accordance with one or more of the requirements set forth in this  
39 subsection; or

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

5 (b) Information originating from, and intermingled to be  
6 indistinguishable with, information under (a) of this subsection that  
7 is maintained by:

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

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

13 (iii) A program or a qualified service organization as defined by  
14 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

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

17 (d) Data maintained for employment records purposes.

18 (3) Processing covered data solely for the purposes expressly  
19 identified in subsection (1) of this section does not, by itself,  
20 make an entity a controller with respect to the processing.

21 (4) If a controller processes covered data pursuant to an  
22 exemption in subsection (1) of this section, the controller bears the  
23 burden of demonstrating that the processing qualifies for the  
24 exemption and complies with the requirements in subsection (2) of  
25 this section.

26 (5)(a) Covered data that is processed by a controller pursuant to  
27 this section must not be processed for any purpose other than those  
28 expressly listed in this section.

29 (b) Covered data that is processed by a controller pursuant to  
30 this section may be processed solely to the extent that such  
31 processing is: (i) Necessary, reasonable, and proportionate to the  
32 purposes listed in this section; (ii) adequate, relevant, and limited  
33 to what is necessary in relation to the specific purpose or purposes  
34 listed in this section; and (iii) insofar as possible, taking into  
35 account the nature and purpose of processing the personal data,  
36 subjected to reasonable administrative, technical, and physical  
37 measures to protect the confidentiality, integrity, and accessibility  
38 of the personal data, and to reduce reasonably foreseeable risks of  
39 harm to consumers.

1        NEW SECTION.    **Sec. 209.**    PRIVATE RIGHT OF ACTION. (1) A violation  
2 of this chapter may not serve as the basis for, or be subject to, a  
3 private right of action under this chapter or under any other law.

4        (2) Rights possessed by consumers as of July 1, 2020, under  
5 chapter 19.86 RCW, the Washington state Constitution, the United  
6 States Constitution, or other laws are not altered.

7        NEW SECTION.    **Sec. 210.**    ENFORCEMENT. (1) This chapter may be  
8 enforced solely by the attorney general under the consumer protection  
9 act, chapter 19.86 RCW.

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

18       (3) The legislative declarations in this section shall not apply  
19 to any claim or action by any party other than the attorney general  
20 alleging that conduct regulated by this chapter violates chapter  
21 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

22       (4) In the event of a controller's or processor's violation under  
23 this chapter, prior to filing a complaint, the attorney general must  
24 provide the controller or processor with a warning letter identifying  
25 the specific provisions of this chapter the attorney general alleges  
26 have been or are being violated. If, after 30 days of issuance of the  
27 warning letter, the attorney general believes the controller or  
28 processor has failed to cure any alleged violation, the attorney  
29 general may bring an action against the controller or processor as  
30 provided under this chapter.

31       (5) A controller or processor found in violation of this chapter  
32 is subject to a civil penalty of up to \$7,500 for each violation.

33       (6) In any action brought under this section, the state is  
34 entitled to recover, in addition to the penalties prescribed in  
35 subsection (5) of this section, the costs of investigation, including  
36 reasonable attorneys' fees.

37       (7) All receipts from the imposition of civil penalties under  
38 this chapter must be deposited into the consumer privacy account  
39 created in section 113 of this act.



1 subsection, contractually obligates any recipients of the information  
2 to comply with all provisions of this subsection.

3 (b) For the purposes of this subsection, the obligations imposed  
4 under (a)(iii) of this subsection do not apply when a controller  
5 discloses deidentified data to the public pursuant to chapter 42.56  
6 RCW or other state disclosure laws.

7 (4) "Delete" means to remove or destroy information such that it  
8 is not maintained in human or machine-readable form and cannot be  
9 retrieved or utilized in the course of business.

10 (5) "Identified or identifiable natural person" means an  
11 individual who can be readily identified, directly or indirectly.

12 (6) "Individual" means a natural person who is a Washington  
13 resident acting only in an individual or household context. It does  
14 not include a natural person acting in a commercial or employment  
15 context.

16 (7) "Institutions of higher education" has the same meaning as  
17 defined in RCW 28B.92.030.

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

19 (9) "Local health departments" has the same meaning as in RCW  
20 70.05.010.

21 (10)(a) "Process," "processed," or "processing" means any  
22 operation or set of operations that are performed on technology-  
23 assisted contact tracing information by automated means, such as the  
24 collection, use, storage, disclosure, analysis, deletion, or  
25 modification of technology-assisted contact tracing information.

26 (b) "Processing" does not include means such as recognized  
27 investigatory measures intended to gather information to facilitate  
28 investigations including, but not limited to, traditional in-person,  
29 email, or telephonic activities used as of the effective date of this  
30 section by the department of health, created under chapter 43.70 RCW,  
31 or local health departments to provide for the control and prevention  
32 of any dangerous, contagious, or infectious disease.

33 (11) "Processor" means a natural or legal person, local  
34 government, state agency, or institutions of higher education that  
35 processes technology-assisted contact tracing information on behalf  
36 of a controller.

37 (12) "Secure" means encrypted in a manner that meets or exceeds  
38 the national institute of standards and technology standard or is  
39 otherwise modified so that the technology-assisted contact tracing

1 information is rendered unreadable, unusable, or undecipherable by an  
2 unauthorized person.

3 (13) "Sell" means the exchange of technology-assisted contact  
4 tracing information for monetary or other valuable consideration by  
5 the controller to a third party. For the purposes of this subsection,  
6 "sell" does not include the recovery of fees by a controller.

7 (14) "State agency" has the same meaning as defined in RCW  
8 43.105.020.

9 (15) "Technology-assisted contact tracing" means the use of a  
10 digital application or other electronic or digital platform that is  
11 capable of independently transmitting information and if offered to  
12 individuals for the purpose of notifying individuals who may have had  
13 contact with an infectious person through data collection and  
14 analysis as a means of controlling the spread of a communicable  
15 disease.

16 (16) "Technology-assisted contact tracing information" means any  
17 information, data, or metadata received through technology-assisted  
18 contact tracing.

19 (17) "Third party" means a natural or legal person, public  
20 authority, agency, or body other than the individual, controller,  
21 processor, or an affiliate of the processor or the controller.

22 NEW SECTION. **Sec. 302.** PROHIBITIONS. Except as provided in this  
23 chapter, it is unlawful for a controller or processor to:

24 (1) Process technology-assisted contact tracing information  
25 unless:

26 (a) The controller or processor provides the individual with a  
27 privacy notice prior to or at the time of the processing; and

28 (b) The individual provides consent for the processing;

29 (2) Disclose any technology-assisted contact tracing information  
30 to federal, state, or local law enforcement;

31 (3) Sell any technology-assisted contact tracing information; or

32 (4) Share any technology-assisted contact tracing information  
33 with another controller, processor, or third party unless the sharing  
34 is governed by a contract or data-sharing agreement as prescribed in  
35 section 303 of this act and is disclosed to an individual in the  
36 notice required in section 304 of this act.

1        NEW SECTION.    **Sec. 303.**    RESPONSIBILITY ACCORDING TO ROLE. (1)

2    Controllers and processors are responsible for meeting their  
3    respective obligations established under this chapter.

4        (2) Processors are responsible under this chapter for adhering to  
5    the instructions of the controller and assisting the controller to  
6    meet its obligations under this chapter. This assistance must include  
7    the processor assisting the controller in meeting the controller's  
8    obligations in relation to the security of processing technology-  
9    assisted contact tracing information and in relation to the  
10   notification of a breach of the security of the system pursuant to  
11   RCW 42.56.590.

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

14        (a) Ensure that each person processing the technology-assisted  
15   contact tracing information is subject to a duty of confidentiality  
16   with respect to the information; and

17        (b) Engage a subcontractor only after providing the controller  
18   with an opportunity to object and pursuant to a written contract in  
19   accordance with subsection (5) of this section that requires the  
20   subcontractor to meet the obligations of the processor with respect  
21   to the technology-assisted contact tracing information.

22        (4) Taking into account the context of processing, the controller  
23   and the processor shall implement appropriate technical and  
24   organizational measures to ensure a level of security appropriate to  
25   the risk and establish a clear allocation of the responsibilities  
26   between them to implement such measures.

27        (5) Processing by a processor must be governed by a contract or  
28   data-sharing agreement between the controller and the processor that  
29   is binding on both parties and that sets out the processing  
30   instructions to which the processor is bound, including the nature  
31   and purpose of the processing, the type of data subject to the  
32   processing, the duration of the processing, and the obligations and  
33   rights of both parties. In addition, the contract or data-sharing  
34   agreement must include the requirements imposed by this subsection  
35   and subsections (3) and (4) of this section, as well as the following  
36   requirements:

37        (a) At the choice of the controller, the processor shall delete  
38   or return all technology-assisted contact tracing information to the  
39   controller as requested at the end of the provision of services,

1 unless retention of the technology-assisted contact tracing  
2 information is required by law;

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

6 (ii) The processor shall allow for, and contribute to, reasonable  
7 audits and inspections by the controller or the controller's  
8 designated auditor. Alternatively, the processor may, with the  
9 controller's consent, arrange for a qualified and independent auditor  
10 to conduct, at least annually and at the processor's expense, an  
11 audit of the processor's policies and technical and organizational  
12 measures in support of the obligations under this chapter using an  
13 appropriate and accepted control standard or framework and audit  
14 procedure for the audits as applicable, and provide a report of the  
15 audit to the controller upon request.

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

20 (7) Determining whether a person is acting as a controller or  
21 processor with respect to a specific processing of data is a fact-  
22 based determination that depends upon the context in which  
23 technology-assisted contact tracing information is to be processed. A  
24 person that is not limited in its processing of technology-assisted  
25 contact tracing information pursuant to a controller's instructions,  
26 or that fails to adhere to such instructions, is a controller and not  
27 a processor with respect to processing of technology-assisted contact  
28 tracing information. A processor that continues to adhere to a  
29 controller's instructions with respect to processing of technology-  
30 assisted contact tracing information remains a processor. If a  
31 processor begins, alone or jointly with others, determining the  
32 purposes and means of the processing of technology-assisted contact  
33 tracing information, it is a controller with respect to the  
34 processing.

35 NEW SECTION. **Sec. 304.** RESPONSIBILITIES OF CONTROLLERS. (1)  
36 Controllers that process technology-assisted contact tracing  
37 information must provide individuals with a clear and conspicuous  
38 privacy notice that includes, at a minimum:

1 (a) The categories of technology-assisted contact tracing  
2 information processed by the controller;

3 (b) The purposes for which the categories of technology-assisted  
4 contact tracing information are processed;

5 (c) The categories of technology-assisted contact tracing  
6 information that the controller shares with third parties, if any;  
7 and

8 (d) The categories of third parties, if any, with whom the  
9 controller shares technology-assisted contact tracing information.

10 (2) A controller's collection of technology-assisted contact  
11 tracing information must be limited to what is reasonably necessary  
12 in relation to the technology-assisted contact tracing purpose for  
13 which the information is processed.

14 (3) A controller's collection of technology-assisted contact  
15 tracing information must be adequate, relevant, and limited to what  
16 is reasonably necessary in relation to the technology-assisted  
17 contact tracing purposes for which the information is processed.

18 (4) Except as provided in this chapter, a controller may not  
19 process technology-assisted contact tracing information for purposes  
20 that are not reasonably necessary to, or compatible with, the  
21 technology-assisted contact tracing purposes for which the  
22 technology-assisted contact tracing information is processed unless  
23 the controller obtains the individual's consent. Controllers may not  
24 process technology-assisted contact tracing information or  
25 deidentified data that was processed for a technology-assisted  
26 contact tracing purpose for purposes of marketing, developing new  
27 products or services, or engaging in commercial product or market  
28 research.

29 (5) A controller shall establish, implement, and maintain  
30 reasonable administrative, technical, and physical data security  
31 practices to protect the confidentiality, integrity, and  
32 accessibility of technology-assisted contact tracing information.  
33 These data security practices must be appropriate to the volume and  
34 nature of the data at issue.

35 (6) A controller must delete or deidentify all technology-  
36 assisted contact tracing information when the information is no  
37 longer being used for a technology-assisted contact tracing purpose  
38 and has met records retention as required by federal or state law.

39 (7) A controller may not process technology-assisted contact  
40 tracing information on the basis of an individual's or a class of

1 individuals' actual or perceived race, color, ethnicity, religion,  
2 national origin, sex, gender, gender identity, sexual orientation,  
3 familial status, lawful source of income, or disability, in a manner  
4 that unlawfully discriminates against the individual or class of  
5 individuals with respect to the offering or provision of: (a)  
6 Housing; (b) employment; (c) credit; (d) education; or (e) the goods,  
7 services, facilities, privileges, advantages, or accommodations of  
8 any place of public accommodation.

9 NEW SECTION. **Sec. 305.** LIMITATIONS AND APPLICABILITY. (1) The  
10 obligations imposed on controllers or processors under this chapter  
11 do not restrict a controller's or processor's ability to:

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

14 (b) Process deidentified information to engage in public or peer-  
15 reviewed scientific, historical, or statistical research in the  
16 public interest that adheres to all other applicable ethics and  
17 privacy laws and is approved, monitored, and governed by an  
18 institutional review board, human subjects research ethics review  
19 board, or a similar independent oversight entity that determines: (i)  
20 If the research is likely to provide substantial benefits that do not  
21 exclusively accrue to the controller; (ii) the expected benefits of  
22 the research outweigh the privacy risks; and (iii) the controller has  
23 implemented reasonable safeguards to mitigate privacy risks  
24 associated with research, including any risks associated with  
25 reidentification.

26 (2) Processing technology-assisted contact tracing information  
27 solely for the purposes expressly identified in this section does  
28 not, by itself, make an entity a controller with respect to such  
29 processing.

30 (3) If a controller processes technology-assisted contact tracing  
31 information pursuant to an exemption in this section, the controller  
32 bears the burden of demonstrating that the processing qualifies for  
33 the exemption and complies with the requirements in subsection (4) of  
34 this section.

35 (4) (a) Technology-assisted contact tracing information that is  
36 processed by a controller pursuant to this section must not be  
37 processed for any purpose other than those expressly listed in this  
38 section.

1 (b) Technology-assisted contact tracing information that is  
2 processed by a controller pursuant to this section may be processed  
3 solely to the extent that such processing is: (i) Necessary,  
4 reasonable, and proportionate to the purposes listed in this section;  
5 (ii) adequate, relevant, and limited to what is necessary in relation  
6 to the specific purpose or purposes listed in this section; and (iii)  
7 insofar as possible, taking into account the nature and purpose of  
8 processing the technology-assisted contact tracing information,  
9 subjected to reasonable administrative, technical, and physical  
10 measures to protect the confidentiality, integrity, and accessibility  
11 of the personal data, and to reduce reasonably foreseeable risks of  
12 harm to consumers.

13 NEW SECTION. **Sec. 306.** LIABILITY. Where more than one  
14 controller or processor, or both a controller and a processor,  
15 involved in the same processing, is in violation of this chapter, the  
16 liability must be allocated among the parties according to principles  
17 of comparative fault.

18 NEW SECTION. **Sec. 307.** ENFORCEMENT. (1) Any waiver of the  
19 provisions of this chapter is contrary to public policy and is void  
20 and unenforceable.

21 (2) (a) Any individual injured by a violation of this chapter may  
22 institute a civil action to recover damages.

23 (b) Any controller that violates, proposes to violate, or has  
24 violated this chapter may be enjoined.

25 (c) The rights and remedies available under this chapter are  
26 cumulative to each other and to any other rights and remedies  
27 available under law.

28 NEW SECTION. **Sec. 308.** EXPIRATION. This chapter expires June  
29 30, 2024.

30 NEW SECTION. **Sec. 309.** If any provision of this act or its  
31 application to any person or circumstance is held invalid, the  
32 remainder of the act or the application of the provision to other  
33 persons or circumstances is not affected.

34 **PART 4**  
35 **Miscellaneous**

1        NEW SECTION.    **Sec. 401.**    (1) Sections 101 through 114 of this act  
2 constitute a new chapter in Title 19 RCW.

3        (2) Sections 201 through 211 of this act constitute a new chapter  
4 in Title 19 RCW.

5        (3) Sections 301 through 308 of this act constitute a new chapter  
6 in Title 43 RCW.

7        NEW SECTION.    **Sec. 402.**    Sections 1, 2, and 101 through 117 of  
8 this act take effect July 31, 2022.

9        NEW SECTION.    **Sec. 403.**    Sections 101 through 114 of this act do  
10 not apply to institutions of higher education or nonprofit  
11 corporations until July 31, 2026.

12        NEW SECTION.    **Sec. 404.**    Except for sections 1, 2, and 101  
13 through 117 of this act, this act is necessary for the immediate  
14 preservation of the public peace, health, or safety, or support of  
15 the state government and its existing public institutions, and takes  
16 effect immediately.

--- END ---