
SECOND SUBSTITUTE SENATE BILL 5062

State of Washington

67th Legislature

2021 Regular Session

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

1 AN ACT Relating to the management, oversight, and use of data;
2 adding a new section to chapter 42.56 RCW; adding a new section to
3 chapter 44.28 RCW; adding new chapters to Title 19 RCW; adding a new
4 chapter to Title 43 RCW; creating new sections; prescribing
5 penalties; providing an effective date; providing expiration dates;
6 and declaring an emergency.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

36 (7) "Consumer" means a natural person who is a Washington
37 resident acting only in an individual or household context. It does
38 not include a natural person acting in a commercial or employment
39 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) "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 (24) "Process" or "processing" means any operation or set of
11 operations which are performed on personal data or on sets of
12 personal data, whether or not by automated means, such as the
13 collection, use, storage, disclosure, analysis, deletion, or
14 modification of personal data.

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

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

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

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

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

34 (30)(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 (31) "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 (32) "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 (33) "State agency" has the same meaning as in RCW 43.105.020.

25 (34) "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 (35) "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) (g)(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, maintained, disclosed, or otherwise
15 used in connection with the gathering, dissemination, or reporting of
16 news or information to the public by news media as defined in RCW
17 5.68.010(5);

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

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

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

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

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

5 (2) A consumer has the right to correct inaccurate personal data
6 concerning the consumer, taking into account the nature of the
7 personal data and the purposes of the processing of the personal
8 data.

9 (3) A consumer has the right to delete personal data concerning
10 the consumer.

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

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

22 NEW SECTION. **Sec. 104.** EXERCISING CONSUMER RIGHTS. (1)
23 Consumers may exercise the rights set forth in section 103 of this
24 act by submitting a request, at any time, to a controller specifying
25 which rights the individual wishes to exercise.

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

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

34 NEW SECTION. **Sec. 105.** RESPONDING TO REQUESTS. (1) Except as
35 provided in this chapter, the controller must comply with a request
36 to exercise the rights pursuant to section 103 of this act.

37 (2) (a) Controllers must provide one or more secure and reliable
38 means for consumers to submit a request to exercise their rights

1 under this chapter. These means must take into account the ways in
2 which consumers interact with the controller and the need for secure
3 and reliable communication of the requests.

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

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

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

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

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

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

39 (5) (a) Controllers must establish an internal process whereby
40 consumers may appeal a refusal to take action on a request to

1 exercise any of the rights under section 103 of this act within a
2 reasonable period of time after the consumer's receipt of the notice
3 sent by the controller under subsection (4)(b) of this section.

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

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

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

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

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

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

1 requests to exercise their rights pursuant to section 103 of this
2 act; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

32 (7) A controller may not discriminate against a consumer for
33 exercising any of the rights contained in this chapter, including
34 denying goods or services to the consumer, charging different prices
35 or rates for goods or services, and providing a different level of
36 quality of goods and services to the consumer. This subsection does
37 not prohibit a controller from offering a different price, rate,
38 level, quality, or selection of goods or services to a consumer,
39 including offering goods or services for no fee, if the offering is
40 in connection with a consumer's voluntary participation in a bona

1 fide loyalty, rewards, premium features, discounts, or club card
2 program. If a consumer exercises their right pursuant to section
3 103(5) of this act, a controller may not sell personal data to a
4 third-party controller as part of such a program unless: (a) The sale
5 is reasonably necessary to enable the third party to provide a
6 benefit to which the consumer is entitled; (b) the sale of personal
7 data to third parties is clearly disclosed in the terms of the
8 program; and (c) the third party uses the personal data only for
9 purposes of facilitating such a benefit to which the consumer is
10 entitled and does not retain or otherwise use or disclose the
11 personal data for any other purpose.

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

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

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

26 (a) Reidentify deidentified data;
27 (b) Comply with an authenticated consumer request to access,
28 correct, delete, or port personal data pursuant to section 103 (1)
29 through (4) of this act, if all of the following are true:

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

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

38 (iii) The controller does not sell the personal data to any third
39 party or otherwise voluntarily disclose the personal data to any

1 third party other than a processor, except as otherwise permitted in
2 this section; or

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

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

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

17 NEW SECTION. **Sec. 109.** DATA PROTECTION ASSESSMENTS. (1)
18 Controllers must conduct and document a data protection assessment of
19 each of the following processing activities involving personal data:

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

22 (b) The processing of personal data for the purposes of the sale
23 of personal data;

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

32 (d) The processing of sensitive data; and

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

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

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

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

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

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

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

36 (b) Comply with a civil, criminal, or regulatory inquiry,
37 investigation, subpoena, or summons by federal, state, local, or
38 other governmental authorities;

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

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

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

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

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

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

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

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

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

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

1 product or service specifically requested by a consumer or the
2 performance of a contract to which the consumer is a party when those
3 internal operations are performed during, and not following, the
4 consumer's relationship with the controller.

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

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

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

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

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

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

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

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

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

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

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

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

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

29 (3) The legislative declarations in this section shall not apply
30 to any claim or action by any party other than the attorney general
31 alleging that conduct regulated by this chapter violates chapter
32 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

33 (4) In the event of a controller's or processor's violation under
34 this chapter, prior to filing a complaint, the attorney general must
35 provide the controller or processor with a warning letter identifying
36 the specific provisions of this chapter the attorney general alleges
37 have been or are being violated. If, after 30 days of issuance of the
38 warning letter, the attorney general believes the controller or

1 processor has failed to cure any alleged violation, the attorney
2 general may bring an action against the controller or processor as
3 provided under this chapter.

4 (5) A controller or processor found in violation of this chapter
5 is subject to a civil penalty of up to \$7,500 for each violation. The
6 civil penalties provided for in this section shall be exclusively
7 assessed and recovered in any action brought by the attorney general
8 under this section.

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

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

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

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

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

32 NEW SECTION. **Sec. 115.** If any provision of this act or its
33 application to any person or circumstance is held invalid, the
34 remainder of the act or the application of the provision to other
35 persons or circumstances is not affected.

1 NEW SECTION. **Sec. 116.** PRIVACY OFFICE REPORT. (1) The state
2 office of privacy and data protection, in collaboration with the
3 office of the attorney general, shall research and examine existing
4 analysis on the development of technology, such as a browser setting,
5 browser extension, or global device setting, indicating a consumer's
6 affirmative, freely given, and unambiguous choice to opt out of the
7 processing of personal data for the purposes of targeted advertising,
8 the sale of personal data, or profiling in furtherance of decisions
9 that produce legal effects concerning consumers or similarly
10 significant effects concerning consumers, and the effectiveness of
11 allowing a consumer to designate a third party to exercise a consumer
12 right on their behalf. A contracted study is not required.

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

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

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

22 NEW SECTION. **Sec. 118.** A new section is added to chapter 44.28
23 RCW to read as follows:

24 (1) By December 1, 2025, the joint committee must review the
25 efficacy of the attorney general providing controllers and processors
26 with warning letters and 30 days to cure alleged violations in the
27 warning letters pursuant to section 112 of this act and report its
28 findings to the governor and the appropriate committees of the
29 legislature.

30 (2) The report must include, but not be limited to:

31 (a) The number of warning letters the attorney general sent to
32 controllers and processors by fiscal year;

33 (b) A list of the controller and processor names that received
34 the warning letters, by fiscal year;

35 (c) The categories of violations and the number of violations per
36 category;

1 (d) The number of actions brought by the attorney general, by
2 fiscal year, as authorized in this act due to a controller or
3 processor not curing the alleged violations within 30 days;

4 (e) The types of resources, including associated costs, expended
5 when providing warning letters and tracking compliance; and

6 (f) A recommendation on whether the warning letters provided by
7 the attorney general should be continued without change or should be
8 amended or repealed, and if so when.

9 (3) The office of the attorney general shall provide the joint
10 committee any data within their purview that the joint committee
11 considers necessary to conduct the review.

12 (4) This section expires June 30, 2026.

13 PART 2

14 Data Privacy Regarding Public Health Emergency—Private Sector

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

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

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

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

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

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

35 (b) "Consumer" does not include a natural person acting in a
36 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) "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 (18) "Personal health data" means information relating to the
9 past, present, or future diagnosis or treatment of a consumer
10 regarding an infectious disease.

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

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

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

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

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

27 (24) "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 (25) "Sell" means the exchange of covered data for monetary or
32 other valuable consideration by the controller to a third party.

33 (26) "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 (27) "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 of a known child, the
34 parent or legal guardian of the known child may exercise the rights
35 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. The
33 civil penalties provided for in this section shall be exclusively
34 assessed and recovered in any action brought by the attorney general
35 under this section.

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

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

4 NEW SECTION. **Sec. 211.** PREEMPTION. (1) Except as provided in
5 this section, this chapter supersedes and preempts laws, ordinances,
6 regulations, or the equivalent adopted by any local entity regarding
7 the processing of covered data for a covered purpose by controllers
8 or processors.

9 (2) Laws, ordinances, or regulations regarding the processing of
10 covered data for a covered purpose by controllers or processors that
11 are adopted by any local entity prior to July 1, 2020, are not
12 superseded or preempted.

13 NEW SECTION. **Sec. 212.** If any provision of this act or its
14 application to any person or circumstance is held invalid, the
15 remainder of the act or the application of the provision to other
16 persons or circumstances is not affected.

17 **PART 3**

18 **Data Privacy Regarding Public Health Emergency—Public Sector**

19 NEW SECTION. **Sec. 301.** The definitions in this section apply
20 throughout this chapter unless the context clearly requires
21 otherwise.

22 (1) "Consent" means a clear affirmative act signifying a freely
23 given, specific, informed, and unambiguous indication of an
24 individual's agreement to the processing of technology-assisted
25 contact tracing information relating to the individual, such as by a
26 written statement, including by electronic means or other clear
27 affirmative action.

28 (2) "Controller" means the local government, state agency, or
29 institutions of higher education that, alone or jointly with others,
30 determines the purposes and means of the processing of technology-
31 assisted contact tracing information.

32 (3) (a) "Deidentified data" means data that cannot reasonably be
33 used to infer information about, or otherwise be linked to, an
34 identified or identifiable natural person, or a device linked to such
35 a person, provided that the controller that possesses the data: (i)
36 Takes reasonable measures to ensure that the data cannot be

1 associated with a natural person; (ii) publicly commits to maintain
2 and use the data only in a deidentified fashion and not attempt to
3 reidentify the data; and (iii) except as provided in (b) of this
4 subsection, contractually obligates any recipients of the information
5 to comply with all provisions of this subsection.

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

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

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

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

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

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

22 (9) "Local health departments" has the same meaning as in RCW
23 70.05.010.

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

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

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

1 (12) "Secure" means encrypted in a manner that meets or exceeds
2 the national institute of standards and technology standard or is
3 otherwise modified so that the technology-assisted contact tracing
4 information is rendered unreadable, unusable, or undecipherable by an
5 unauthorized person.

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

10 (14) "State agency" has the same meaning as defined in RCW
11 43.105.020.

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

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

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

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

27 (1) Process technology-assisted contact tracing information
28 unless:

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

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

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

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

35 (4) Share any technology-assisted contact tracing information
36 with another controller, processor, or third party unless the sharing
37 is governed by a contract or data-sharing agreement as prescribed in
38 section 303 of this act and is disclosed to an individual in the
39 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
35

PART 4
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 118 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 ---