
SENATE BILL 5062

State of Washington

67th Legislature

2021 Regular Session

By Senators Carlyle and Nguyen

Prefiled 01/05/21.

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

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

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

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

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

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

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

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

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

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

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

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

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

30 (9) Lastly, the legislature encourages the state office of
31 privacy and data protection to monitor the development of universal
32 privacy controls that communicate a consumer's affirmative, freely
33 given, and unambiguous choice to opt out of the processing of their
34 personal data.

35 **PART 1**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

35 (19) "Legislative agencies" has the same meaning as defined in
36 RCW 44.80.020.

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

38 (21) "Nonprofit corporation" has the same meaning as in RCW
39 24.03.005.

1 (22) (a) "Personal data" means any information that is linked or
2 reasonably linkable to an identified or identifiable natural person.
3 "Personal data" does not include deidentified data or publicly
4 available information.

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

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

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

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

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

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

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

32 (b) "Sale" does not include the following: (i) The disclosure of
33 personal data to a processor who processes the personal data on
34 behalf of the controller; (ii) the disclosure of personal data to a
35 third party with whom the consumer has a direct relationship for
36 purposes of providing a product or service requested by the consumer;
37 (iii) the disclosure or transfer of personal data to an affiliate of
38 the controller; (iv) the disclosure of information that the consumer
39 (A) intentionally made available to the general public via a channel
40 of mass media, and (B) did not restrict to a specific audience; or

1 (v) the disclosure or transfer of personal data to a third party as
2 an asset that is part of a merger, acquisition, bankruptcy, or other
3 transaction in which the third party assumes control of all or part
4 of the controller's assets.

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

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

19 (31) "State agency" has the same meaning as in RCW 43.105.020.

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

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

33 NEW SECTION. **Sec. 102.** JURISDICTIONAL SCOPE. (1) This chapter
34 applies to legal entities that conduct business in Washington or
35 produce products or services that are targeted to residents of
36 Washington, and that satisfy one or more of the following thresholds:

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

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

4 (2) This chapter does not apply to:

5 (a) State agencies, legislative agencies, local governments, or
6 tribes;

7 (b) Municipal corporations;

8 (c) Information that meets the definition of:

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

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

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

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

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

26 (A) A quality improvement committee for purposes of RCW
27 43.70.510, 70.230.080, or 70.41.200;

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

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

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

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

38 (vii) Patient safety work product for purposes of 42 C.F.R. Part
39 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26; or

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

5 (d) Information originating from, and intermingled to be
6 indistinguishable with, information under (c) 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 (e) Information used only for public health activities and
16 purposes as described in 45 C.F.R. Sec. 164.512;

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

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

34 (g) Personal data collected and maintained for purposes of
35 chapter 43.71 RCW;

36 (h) Personal data collected, processed, sold, or disclosed
37 pursuant to the federal Gramm-Leach-Bliley act (P.L. 106-102), and
38 implementing regulations, if the collection, processing, sale, or
39 disclosure is in compliance with that law;

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

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

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

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

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

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

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

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

36 (2) A consumer has the right to correct inaccurate personal data
37 concerning the consumer, taking into account the nature of the
38 personal data and the purposes of the processing of the personal
39 data.

1 (3) A consumer has the right to delete personal data concerning
2 the consumer.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 notification of a breach of the security of the system pursuant to
2 RCW 19.255.010; and provide information to the controller necessary
3 to enable the controller to conduct and document any data protection
4 assessments required by section 109 of this act.

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

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

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

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

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

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

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

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

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

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

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

20 NEW SECTION. **Sec. 107.** RESPONSIBILITIES OF CONTROLLERS. (1)(a)

21 Controllers shall provide consumers with a reasonably accessible,
22 clear, and meaningful privacy notice that includes:

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

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

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

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

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

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

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

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

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

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

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

25 (7) A controller may not discriminate against a consumer for
26 exercising any of the rights contained in this chapter, including
27 denying goods or services to the consumer, charging different prices
28 or rates for goods or services, and providing a different level of
29 quality of goods and services to the consumer. This subsection does
30 not prohibit a controller from offering a different price, rate,
31 level, quality, or selection of goods or services to a consumer,
32 including offering goods or services for no fee, if the offering is
33 in connection with a consumer's voluntary participation in a bona
34 fide loyalty, rewards, premium features, discounts, or club card
35 program. A controller may not sell personal data to a third-party
36 controller as part of such a program unless: (a) The sale is
37 reasonably necessary to enable the third party to provide a benefit
38 to which the consumer is entitled; (b) the sale of personal data to
39 third parties is clearly disclosed in the terms of the program; and
40 (c) the third party uses the personal data only for purposes of

1 facilitating such a benefit to which the consumer is entitled and
2 does not retain or otherwise use or disclose the personal data for
3 any other purpose.

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

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

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

18 (a) Reidentify deidentified data;

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

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

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

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

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

37 (2) The rights contained in section 103 (1) through (4) of this
38 act do not apply to pseudonymous data in cases where the controller
39 is able to demonstrate any information necessary to identify the

1 consumer is kept separately and is subject to effective technical and
2 organizational controls that prevent the controller from accessing
3 such information.

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

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

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

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

14 (b) The processing of personal data for the purposes of the sale
15 of personal data;

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

24 (d) The processing of sensitive data; and

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

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

31 (2) Data protection assessments conducted under subsection (1) of
32 this section must identify and weigh the benefits that may flow
33 directly and indirectly from the processing to the controller,
34 consumer, other stakeholders, and the public against the potential
35 risks to the rights of the consumer associated with such processing,
36 as mitigated by safeguards that can be employed by the controller to
37 reduce such risks. The use of deidentified data and the reasonable
38 expectations of consumers, as well as the context of the processing
39 and the relationship between the controller and the consumer whose

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

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

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

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

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

27 (b) Comply with a civil, criminal, or regulatory inquiry,
28 investigation, subpoena, or summons by federal, state, local, or
29 other governmental authorities;

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

34 (d) Investigate, establish, exercise, prepare for, or defend
35 legal claims;

36 (e) Provide a product or service specifically requested by a
37 consumer, perform a contract to which the consumer is a party, or
38 take steps at the request of the consumer prior to entering into a
39 contract;

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

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

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

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

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

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

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

35 (3) The obligations imposed on controllers or processors under
36 this chapter do not apply where compliance by the controller or
37 processor with this chapter would violate an evidentiary privilege
38 under Washington law and do not prevent a controller or processor
39 from providing personal data concerning a consumer to a person

1 covered by an evidentiary privilege under Washington law as part of a
2 privileged communication.

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

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

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

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

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

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

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

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

1 of the personal data, and to reduce reasonably foreseeable risks of
2 harm to consumers.

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

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

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

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

20 (3) The legislative declarations in this section shall not apply
21 to any claim or action by any party other than the attorney general
22 alleging that conduct regulated by this chapter violates chapter
23 19.86 RCW, and this chapter does not incorporate RCW 19.86.093.

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

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

35 (6) In any action brought under this section, the state is
36 entitled to recover, in addition to the penalties prescribed in
37 subsection (5) of this section, the costs of investigation, including
38 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. 113.** CONSUMER PRIVACY ACCOUNT. The consumer
5 privacy account is created in the state treasury. All receipts from
6 the imposition of civil penalties under this chapter must be
7 deposited into the account. Moneys in the account may be spent only
8 after appropriation. Moneys in the account may only be used for the
9 purposes of recovery of costs and attorneys' fees accrued by the
10 attorney general in enforcing this chapter and for the office of
11 privacy and data protection as created in RCW 43.105.369. Moneys may
12 not be used to supplant general fund appropriations to either agency.

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

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

20 NEW SECTION. **Sec. 115.** If any provision of this act or its
21 application to any person or circumstance is held invalid, the
22 remainder of the act or the application of the provision to other
23 persons or circumstances is not affected.

24 NEW SECTION. **Sec. 116.** PRIVACY OFFICE REPORT. (1) The state
25 office of privacy and data protection, in collaboration with the
26 office of the attorney general, shall research and examine existing
27 analysis on the development of technology, such as a browser setting,
28 browser extension, or global device setting, indicating a consumer's
29 affirmative, freely given, and unambiguous choice to opt out of the
30 processing of personal data for the purposes of targeted advertising,
31 the sale of personal data, or profiling in furtherance of decisions
32 that produce legal effects concerning consumers or similarly
33 significant effects concerning consumers. A contracted study is not
34 required.

35 (2) The office of privacy and data protection shall submit a
36 report of its findings and will identify specific recommendations to

1 the governor and the appropriate committees of the legislature by
2 December 1, 2022.

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

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

8 **PART 2**
9 **Data Privacy Regarding Public Health Emergency—Private Sector**

10 NEW SECTION. **Sec. 201.** The definitions in this section apply
11 throughout this chapter unless the context clearly requires
12 otherwise.

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

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

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

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

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

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

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

35 (7) "Covered data" includes personal data and one or more of the
36 following: Specific geolocation data; proximity data; or personal
37 health data.

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

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

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

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

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

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

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

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

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

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

1 "Personal data" does not include deidentified data or publicly
2 available information.

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

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

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

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

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

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

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

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

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

35 (26) "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. 202.** PROHIBITIONS. Except as provided in this
39 chapter, it is unlawful for a controller or processor to:

1 (1) Process covered data for a covered purpose unless:
2 (a) The controller or processor provides the consumer with a
3 privacy notice as required in section 207 of this act prior to or at
4 the time of the processing; and
5 (b) The consumer provides consent for the processing;
6 (2) Disclose any covered data processed for a covered purpose to
7 federal, state, or local law enforcement;
8 (3) Sell any covered data processed for a covered purpose; or
9 (4) Share any covered data processed for a covered purpose with
10 another controller, processor, or third party unless the sharing is
11 governed by contract pursuant to section 206 of this act and is
12 disclosed to a consumer in the notice required in section 207 of this
13 act.

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

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

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

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

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

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

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

36 NEW SECTION. **Sec. 205.** RESPONDING TO REQUESTS. (1) Except as
37 provided in this chapter, controllers that process covered data for a

1 covered purpose must comply with a request to exercise the rights
2 pursuant to section 203 of this act.

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

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

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

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

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

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

36 (d) A controller is not required to comply with a request to
37 exercise any of the rights under section 203 (1) through (4) of this
38 act if the controller is unable to authenticate the request using
39 commercially reasonable efforts. In such a case, the controller may

1 request the provision of additional information reasonably necessary
2 to authenticate the request.

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

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

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

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

33 NEW SECTION. **Sec. 206.** RESPONSIBILITY ACCORDING TO ROLE. (1)
34 Controllers and processors are responsible for meeting their
35 respective obligations established under this chapter.

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

1 (a) Taking into account the nature of the processing, the
2 processor shall assist the controller by appropriate technical and
3 organizational measures, insofar as this is possible, for the
4 fulfillment of the controller's obligation to respond to consumer
5 requests to exercise their rights pursuant to section 203 of this
6 act; and

7 (b) Taking into account the nature of processing and the
8 information available to the processor, the processor shall: Assist
9 the controller in meeting the controller's obligations in relation to
10 the security of processing the personal data and in relation to the
11 notification of a breach of the security of the system pursuant to
12 RCW 19.255.010; and provide information to the controller necessary
13 to enable the controller to conduct and document any data protection
14 assessments required by section 109 of this act.

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

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

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

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

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

38 (a) At the choice of the controller, the processor shall delete
39 or return all personal data to the controller as requested at the end

1 of the provision of services, unless retention of the personal data
2 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 relieve a controller or a
17 processor from the liabilities imposed on them by virtue of its role
18 in the processing relationship as defined by this chapter.

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

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

35 (a) How a consumer may exercise the rights contained in section
36 203 of this act, including how a consumer may appeal a controller's
37 action with regard to the consumer's request;

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

1 (c) The purposes for which the categories of covered data are
2 processed;

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

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

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

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

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

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

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

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

38 (8) Any provision of a contract or agreement of any kind that
39 purports to waive or limit in any way a consumer's rights under this

1 chapter is deemed contrary to public policy and is void and
2 unenforceable.

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

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

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

20 (2) This chapter does not apply to:

21 (a) Information that meets the definition of:

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

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

27 (iii) Identifiable private information for purposes of the
28 federal policy for the protection of human subjects, 45 C.F.R. Part
29 46; identifiable private information that is otherwise information
30 collected as part of human subjects research pursuant to the good
31 clinical practice guidelines issued by the international council for
32 harmonization; the protection of human subjects under 21 C.F.R. Parts
33 50 and 56; or personal data used or shared in research conducted in
34 accordance with one or more of the requirements set forth in this
35 subsection; or

36 (iv) Information that is (A) deidentified in accordance with the
37 requirements for deidentification set forth in 45 C.F.R. Sec. 102,
38 and (B) derived from any of the health care-related information
39 listed in this subsection (2)(a);

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

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

7 (ii) A health care facility or health care provider as defined in
8 RCW 70.02.010; or

9 (iii) A program or a qualified service organization as defined by
10 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

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

13 (d) Data maintained for employment records purposes.

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

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

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

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

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

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

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

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

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

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

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

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

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

37 NEW SECTION. **Sec. 211.** PREEMPTION. (1) Except as provided in
38 this section, this chapter supersedes and preempts laws, ordinances,

1 regulations, or the equivalent adopted by any local entity regarding
2 the processing of covered data for a covered purpose by controllers
3 or processors.

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

8 NEW SECTION. **Sec. 212.** If any provision of this act or its
9 application to any person or circumstance is held invalid, the
10 remainder of the act or the application of the provision to other
11 persons or circumstances is not affected.

12 **PART 3**

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

14 NEW SECTION. **Sec. 301.** The definitions in this section apply
15 throughout this chapter unless the context clearly requires
16 otherwise.

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

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

27 (3) (a) "Deidentified data" means data that cannot reasonably be
28 used to infer information about, or otherwise be linked to, an
29 identified or identifiable natural person, or a device linked to such
30 a person, provided that the controller that possesses the data: (i)
31 Takes reasonable measures to ensure that the data cannot be
32 associated with a natural person; (ii) publicly commits to maintain
33 and use the data only in a deidentified fashion and not attempt to
34 reidentify the data; and (iii) except as provided in (b) of this
35 subsection, contractually obligates any recipients of the information
36 to comply with all provisions of this subsection.

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

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

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

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

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

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

17 (9) "Local health departments" has the same meaning as in RCW
18 70.05.010.

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

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

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

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

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

5 (14) "State agency" has the same meaning as defined in RCW
6 43.105.020.

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

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

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

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

22 (1) Process technology-assisted contact tracing information
23 unless:

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

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

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

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

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

35 NEW SECTION. **Sec. 303.** RESPONSIBILITY ACCORDING TO ROLE. (1)
36 Controllers and processors are responsible for meeting their
37 respective obligations established under this chapter.

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

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

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

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

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

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

34 (a) At the choice of the controller, the processor shall delete
35 or return all technology-assisted contact tracing information to the
36 controller as requested at the end of the provision of services,
37 unless retention of the technology-assisted contact tracing
38 information 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 or data-sharing agreement
15 relieve a controller or a processor from the liabilities imposed on
16 them by virtue of its role in the processing relationship as defined
17 in this chapter.

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

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

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

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

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

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

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

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

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

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

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

37 (7) A controller may not process technology-assisted contact
38 tracing information on the basis of an individual's or a class of
39 individuals' actual or perceived race, color, ethnicity, religion,
40 national origin, sex, gender, gender identity, sexual orientation,

1 familial status, lawful source of income, or disability, in a manner
2 that unlawfully discriminates against the individual or class of
3 individuals with respect to the offering or provision of: (a)
4 Housing; (b) employment; (c) credit; (d) education; or (e) the goods,
5 services, facilities, privileges, advantages, or accommodations of
6 any place of public accommodation.

7 NEW SECTION. **Sec. 305.** 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) the controller has
21 implemented reasonable safeguards to mitigate privacy risks
22 associated with research, including any risks associated with
23 reidentification.

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

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

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

37 (b) Technology-assisted contact tracing information that is
38 processed by a controller pursuant to this section may be processed
39 solely to the extent that such processing is: (i) Necessary,

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

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

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

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

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

22 (c) The rights and remedies available under this chapter are
23 cumulative to each other and to any other rights and remedies
24 available under law.

25 NEW SECTION. **Sec. 308.** EXPIRATION. This chapter expires June
26 30, 2024.

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

31 **PART 4**
32 **Miscellaneous**

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

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

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

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

7 NEW SECTION. **Sec. 403.** This chapter does not apply to
8 institutions of higher education, air carriers, or nonprofit
9 corporations until July 31, 2026.

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

--- END ---