<div align="right">By Representative Hansen</div>

1   Strike everything after the enacting clause and insert the
2 following:

3   "<u>NEW SECTION.</u> **Sec. 1.** SHORT TITLE. This act may be known and
4 cited as the Washington privacy act.

5   <u>NEW SECTION.</u> **Sec. 2.** LEGISLATIVE FINDINGS AND INTENT. (1) The
6 legislature finds that the people of Washington regard their privacy
7 as a fundamental right and an essential element of their individual
8 freedom. Washington's Constitution explicitly provides the right to
9 privacy, and fundamental privacy rights have long been and continue
10 to be integral to protecting Washingtonians and to safeguarding our
11 democratic republic.
12   (2) Ongoing advances in technology have produced an exponential
13 growth in the volume and variety of personal data being generated,
14 collected, stored, and analyzed, which presents both promise and
15 potential peril. The ability to harness and use data in positive ways
16 is driving innovation and brings beneficial technologies to society.
17 However, it has also created risks to privacy and freedom. The
18 unregulated and unauthorized use and disclosure of personal
19 information and loss of privacy can have devastating impacts, ranging
20 from financial fraud, identity theft, and unnecessary costs, to
21 personal time and finances, to destruction of property, harassment,
22 reputational damage, emotional distress, and physical harm.
23   (3) Given that technological innovation and new uses of data can
24 help solve societal problems, protect public health associated with
25 global pandemics, and improve quality of life, the legislature seeks
26 to shape responsible public policies where innovation and protection
27 of individual privacy coexist. The legislature notes that our federal
28 authorities have not developed or adopted into law regulatory or
29 legislative solutions that give consumers control over their privacy.
30 In contrast, the European Union's general data protection regulation

1 has continued to influence data privacy policies and practices of
2 those businesses competing in global markets. In the absence of
3 federal standards, Washington and other states across the United
4 States are analyzing elements of the European Union's general data
5 protection regulation to enact state-based data privacy regulatory
6 protections.

7   (4) Responding to COVID-19 illustrates the need for public
8 policies that protect individual privacy while fostering
9 technological innovation. For years, contact tracing best practices
10 have been used by public health officials to securely process high
11 value individual data and have effectively stopped the prolific
12 spread of infectious diseases. However, the scale of COVID-19 is
13 unprecedented. Contact tracing is evolving in a manner that
14 necessitates the use of technology to rapidly collect and process
15 data from multiple data sets, many of which are unanticipated, to
16 protect public health as well as to facilitate the continued safe
17 operation of the economy. The benefits of such technology, however,
18 should not supersede the potential privacy risks to individuals.

19   (5) Exposure notification applications have already been deployed
20 throughout the country and the world. However, contact tracing
21 technology is rapidly evolving. Applications may be integrated in a
22 manner that facilitates the aggregation and sharing of individual
23 data that in effect generate profiles of individuals. Artificial
24 intelligence may be used for the extrapolation of data to analyze and
25 interpret data for public health purposes. Moreover, the potential
26 government use of exposure notification applications poses additional
27 potential privacy risks to individuals due to the types of sensitive
28 data it has access to and processes. Much of that processing may have
29 legal effects, including access to services or establishments. The
30 capabilities of next generation contact tracing technologies are
31 unknown and policies must be in place to provide privacy protections
32 for current uses as well as potential future uses.

33   (6) With this act, the legislature intends to: Provide a modern
34 privacy regulatory framework with data privacy guardrails to protect
35 individual privacy; establish mechanisms for consumers to exercise
36 control over their data; instill public confidence on the processing
37 of their personal and public health data during any global pandemic;
38 and require companies to be responsible custodians of data as
39 technological innovations emerge.

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

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

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

PART 1

Personal Data Privacy Regulations—Private Sector

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

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

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

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

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

11   (5) "Child" has the same meaning as defined in the children's
12   online privacy protection act, Title 15 U.S.C. Sec. 6501 through
13   6506.

14   (6) "Consent" means any freely given, specific, informed, and
15   unambiguous indication of the consumer's wishes by which the consumer
16   signifies agreement to the processing of personal data relating to
17   the consumer for a narrowly defined particular purpose. Acceptance of
18   a general or broad terms of use or similar document that contains
19   descriptions of personal data processing along with other, unrelated
20   information, does not constitute consent. Hovering over, muting,
21   pausing, or closing a given piece of content does not constitute
22   consent. Likewise, agreement obtained through dark patterns does not
23   constitute consent.

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

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

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

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

37   (11) "Decisions that produce legal effects concerning a consumer
38   or similarly significant effects concerning a consumer" means
39   decisions that result in the provision or denial of financial and
40   lending services, housing, insurance, education enrollment, criminal

justice, employment opportunities, health care services, or access to
basic necessities, such as food and water.

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

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

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

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

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

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

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

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

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

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

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

(23) "Nonprofit corporation" has the same meaning as in RCW
24.03.005.

(24) "Personal data" means any information, including
pseudonymous data, that is linked or reasonably linkable to an
identified or identifiable natural person. "Personal data" does not
include deidentified data or publicly available information.

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

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

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

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

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

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

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

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

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

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

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

(35) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from a consumer's activities over time and across one or more distinctly branded websites or online applications to predict the consumer's preferences or interests. It does not include advertising: (a) Based on activities within a controller's own commonly branded websites or online applications; (b) based on the context of a consumer's current search query or visit to a website or online application; or (c) to a consumer in response to the consumer's request for information or feedback.

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

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

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

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

(2) This chapter does not apply to:

1   (a) State agencies, legislative agencies, the judicial branch,
2 local governments, or tribes;

3   (b) Municipal corporations;

4   (c) Air carriers;

5   (d) Nonprofit organizations that:

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

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

10   (iii) Do not sell personal data collected by the organization;

11   (e) Information that meets the definition of:

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

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

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

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

27   (v) Information and documents created specifically for, and
28 collected and maintained by:

29   (A) A quality improvement committee for purposes of RCW
30 43.70.510, 70.230.080, or 70.41.200;

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

32   (C) A quality assurance committee for purposes of RCW 74.42.640
33 or 18.20.390;

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

38   (vi) Information and documents created for purposes of the
39 federal health care quality improvement act of 1986, and related
40 regulations;

1   (vii) Patient safety work product for purposes of 42 C.F.R. Part
2 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26; or
3   (viii) Information that is (A) deidentified in accordance with
4 the requirements for deidentification set forth in 45 C.F.R. Part
5 164, and (B) derived from any of the health care-related information
6 listed in this subsection (2)(e);
7   (f) Information originating from, and intermingled to be
8 indistinguishable with, information under (e) of this subsection that
9 is maintained by:
10   (i) A covered entity or business associate as defined by the
11 health insurance portability and accountability act of 1996 and
12 related regulations;
13   (ii) A health care facility or health care provider as defined in
14 RCW 70.02.010; or
15   (iii) A program or a qualified service organization as defined by
16 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;
17   (g) Information used only for public health activities and
18 purposes as described in 45 C.F.R. Sec. 164.512;
19   (h)(i) An activity involving the collection, maintenance,
20 disclosure, sale, communication, or use of any personal data bearing
21 on a consumer's credit worthiness, credit standing, credit capacity,
22 character, general reputation, personal characteristics, or mode of
23 living by a consumer reporting agency, as defined in Title 15 U.S.C.
24 Sec. 1681a(f), by a furnisher of information, as set forth in Title
25 15 U.S.C. Sec. 1681s-2, who provides information for use in a
26 consumer report, as defined in Title 15 U.S.C. Sec. 1681a(d), and by
27 a user of a consumer report, as set forth in Title 15 U.S.C. Sec.
28 1681b.
29   (ii) (h)(i) of this subsection applies only to the extent that
30 such an activity involving the collection, maintenance, disclosure,
31 sale, communication, or use of such personal data by that agency,
32 furnisher, or user is subject to regulation under the fair credit
33 reporting act, Title 15 U.S.C. Sec. 1681 et seq., and the personal
34 data is not collected, maintained, used, communicated, disclosed, or
35 sold except as authorized by the fair credit reporting act;
36   (i) Personal data collected and maintained for purposes of
37 chapter 43.71 RCW;
38   (j) Personal data collected, processed, sold, or disclosed
39 pursuant to the federal Gramm-Leach-Bliley act (P.L. 106-102), and

1 implementing regulations, if the collection, processing, sale, or
2 disclosure is in compliance with that law;

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

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

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

12   (n) Personal data collected, maintained, disclosed, or otherwise
13 used in connection with the gathering, dissemination, or reporting of
14 news or information to the public by news media as defined in RCW
15 5.68.010(5);

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

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

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

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

38   NEW SECTION. **Sec. 103.** CONSUMER RIGHTS. (1) A consumer has the
39 right to confirm whether or not a controller is processing personal

data concerning the consumer and access the personal data the controller is processing.

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

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

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

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

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

(2) Beginning July 31, 2023, a consumer may exercise the rights under section 103(5) (a) and (b) of this act:

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

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

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

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

1   NEW SECTION. **Sec. 105.** RESPONDING TO REQUESTS. (1) Except as
2   provided in this chapter, the controller must comply with a request
3   to exercise the rights pursuant to section 103 of this act.
4   (2)(a) Controllers must provide one or more secure and reliable
5   means for consumers to submit a request to exercise their rights
6   under this chapter. These means must take into account the ways in
7   which consumers interact with the controller and the need for secure
8   and reliable communication of the requests.
9   (b) Controllers may not require a consumer to create a new
10   account in order to exercise a right, but a controller may require a
11   consumer to use an existing account to exercise the consumer's rights
12   under this chapter.
13   (3) A controller must comply with a request to exercise the right
14   in section 103(5) of this act as soon as feasibly possible, but no
15   later than 15 days of receipt of the request.
16   (4)(a) A controller must inform a consumer of any action taken on
17   a request to exercise any of the rights in section 103 (1) through
18   (4) of this act without undue delay and in any event within 45 days
19   of receipt of the request. That period may be extended once by 45
20   additional days where reasonably necessary, taking into account the
21   complexity and number of the requests. The controller must inform the
22   consumer of any such extension within 45 days of receipt of the
23   request, together with the reasons for the delay.
24   (b) If a controller does not take action on the request of a
25   consumer, the controller must inform the consumer without undue delay
26   and at the latest within 45 days of receipt of the request of the
27   reasons for not taking action and instructions for how to appeal the
28   decision with the controller as described in subsection (5) of this
29   section.
30   (c) Information provided under this section must be provided by
31   the controller to the consumer free of charge, up to twice annually.
32   Where requests from a consumer are manifestly unfounded or excessive,
33   in particular because of their repetitive character, the controller
34   may either: (i) Charge a reasonable fee to cover the administrative
35   costs of complying with the request; or (ii) refuse to act on the
36   request. The controller bears the burden of demonstrating the
37   manifestly unfounded or excessive character of the request.
38   (d) A controller is not required to comply with a request to
39   exercise any of the rights under section 103 (1) through (4) of this
40   act if the controller is unable to authenticate the request using

1 commercially reasonable efforts. In such a case, the controller may
2 request the provision of additional information reasonably necessary
3 to authenticate the request.

4 (5)(a) A controller must establish an internal process whereby a
5 consumer may appeal a refusal to take action on a request to exercise
6 any of the rights under section 103 of this act within a reasonable
7 period of time after the controller refuses to take action on such
8 request.

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

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

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

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

37 (2) Processors are responsible under this chapter for adhering to
38 the instructions of the controller and assisting the controller to

meet its obligations under this chapter. This assistance includes the following:

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

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

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

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

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

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

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

1   imposed by this subsection and subsections (3) and (4) of this
 2   section, as well as the following requirements:
 3   (a) At the choice of the controller, the processor shall delete
 4   or return all personal data to the controller as requested at the end
 5   of the provision of services, unless retention of the personal data
 6   is required by law;
 7   (b)(i) The processor shall make available to the controller all
 8   information necessary to demonstrate compliance with the obligations
 9   in this chapter; and
10   (ii) The processor shall allow for, and contribute to, reasonable
11   audits and inspections by the controller or the controller's
12   designated auditor. Alternatively, the processor may, with the
13   controller's consent, arrange for a qualified and independent auditor
14   to conduct, at least annually and at the processor's expense, an
15   audit of the processor's policies and technical and organizational
16   measures in support of the obligations under this chapter using an
17   appropriate and accepted control standard or framework and audit
18   procedure for the audits as applicable, and provide a report of the
19   audit to the controller upon request.
20   (6) In no event may any contract relieve a controller or a
21   processor from the liabilities imposed on them by virtue of its role
22   in the processing relationship as defined by this chapter.
23   (7) Determining whether a person is acting as a controller or
24   processor with respect to a specific processing of data is a fact-
25   based determination that depends upon the context in which personal
26   data are to be processed. A person that is not limited in its
27   processing of personal data pursuant to a controller's instructions,
28   or that fails to adhere to such instructions, is a controller and not
29   a processor with respect to a specific processing of data. A
30   processor that continues to adhere to a controller's instructions
31   with respect to a specific processing of personal data remains a
32   processor. If a processor begins, alone or jointly with others,
33   determining the purposes and means of the processing of personal
34   data, it is a controller with respect to the processing.

35   NEW SECTION. **Sec. 107.** RESPONSIBILITIES OF CONTROLLERS. (1)(a)
36   Controllers shall provide consumers with a reasonably accessible,
37   clear, and meaningful privacy notice that includes:
38   (i) The categories of personal data processed by the controller;

1   (ii) The purposes for which the categories of personal data are
2 processed;
3   (iii) How and where consumers may exercise the rights contained
4 in section 103 of this act, including how a consumer may appeal a
5 controller's action with regard to the consumer's request;
6   (iv) The categories of personal data that the controller shares
7 with third parties, if any; and
8   (v) The categories of third parties, if any, with whom the
9 controller shares personal data.
10   (b) If a controller sells personal data to third parties or
11 processes personal data for targeted advertising, the controller must
12 clearly and conspicuously disclose the processing, as well as the
13 manner in which a consumer may exercise the right to opt out of the
14 processing, in a clear and conspicuous manner.
15   (c) The privacy notice required under this subsection must:
16   (i) Use clear and plain language;
17   (ii) Be in English and any other language in which a controller
18 communicates with the consumer to whom the information pertains; and
19   (iii) Be understandable to the least sophisticated consumer.
20   (2) A controller's collection of personal data must be limited to
21 what is reasonably necessary in relation to the purposes for which
22 the data is processed.
23   (3) A controller's collection of personal data must be adequate,
24 relevant, and limited to what is reasonably necessary in relation to
25 the purposes for which the data is processed.
26   (4) Except as provided in this chapter, a controller may not
27 process personal data for purposes that are not reasonably necessary
28 to, or compatible with, the purposes for which the personal data is
29 processed unless the controller obtains the consumer's consent.
30   (5) A controller shall establish, implement, and maintain
31 reasonable administrative, technical, and physical data security
32 practices to protect the confidentiality, integrity, and
33 accessibility of personal data. The data security practices must be
34 appropriate to the volume and nature of the personal data at issue.
35   (6) A controller shall not process personal data on the basis of
36 a consumer's or a class of consumers' actual or perceived race,
37 color, ethnicity, religion, national origin, sex, gender, gender
38 identity, sexual orientation, familial status, lawful source of
39 income, or disability, in a manner that unlawfully discriminates
40 against the consumer or class of consumers with respect to the

1 offering or provision of: (a) Housing; (b) employment; (c) credit;
2 (d) education; or (e) the goods, services, facilities, privileges,
3 advantages, or accommodations of any place of public accommodation.

4 (7) A controller may not discriminate against a consumer for
5 exercising any of the rights contained in this chapter, including
6 denying goods or services to the consumer, charging different prices
7 or rates for goods or services, and providing a different level of
8 quality of goods and services to the consumer. This subsection does
9 not prohibit a controller from offering a different price, rate,
10 level, quality, or selection of goods or services to a consumer,
11 including offering goods or services for no fee, if the offering is
12 in connection with a consumer's voluntary participation in a bona
13 fide loyalty, rewards, premium features, discounts, or club card
14 program. If a consumer exercises their right pursuant to section
15 103(5) of this act, a controller may not sell personal data to a
16 third-party controller as part of such a program unless: (a) The sale
17 is reasonably necessary to enable the third party to provide a
18 benefit to which the consumer is entitled; (b) the sale of personal
19 data to third parties is clearly disclosed in the terms of the
20 program; and (c) the third party uses the personal data only for
21 purposes of facilitating such a benefit to which the consumer is
22 entitled and does not retain or otherwise use or disclose the
23 personal data for any other purpose.

24 (8) Except as otherwise provided in this chapter, a controller
25 may not process sensitive data concerning a consumer without
26 obtaining the consumer's consent or, in the case of the processing of
27 sensitive data of a known child, without obtaining consent from the
28 child's parent or lawful guardian, in accordance with the children's
29 online privacy protection act requirements.

30 (9) Except as otherwise provided in this chapter, a controller
31 may not process the personal data of a minor for the purposes of
32 targeted advertising or the sale of personal data without obtaining
33 consent from the minor.

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

38 NEW SECTION. **Sec. 108.** PROCESSING DEIDENTIFIED DATA OR
39 PSEUDONYMOUS DATA. (1) This chapter does not require a controller or

1 processor to do any of the following solely for purposes of complying
2 with this chapter:
3 (a) Reidentify deidentified data;
4 (b) Comply with an authenticated consumer request to access,
5 correct, delete, or port personal data pursuant to section 103 (1)
6 through (4) of this act, if all of the following are true:
7 (i)(A) The controller is not reasonably capable of associating
8 the request with the personal data; or (B) it would be unreasonably
9 burdensome for the controller to associate the request with the
10 personal data;
11 (ii) The controller does not use the personal data to recognize
12 or respond to the specific consumer who is the subject of the
13 personal data, or associate the personal data with other personal
14 data about the same specific consumer; and
15 (iii) The controller does not sell the personal data to any third
16 party or otherwise voluntarily disclose the personal data to any
17 third party other than a processor, except as otherwise permitted in
18 this section; or
19 (c) Maintain data in identifiable form, or collect, obtain,
20 retain, or access any data or technology, in order to be capable of
21 associating an authenticated consumer request with personal data.
22 (2) The rights contained in section 103 (1) through (4) of this
23 act do not apply to pseudonymous data in cases where the controller
24 is able to demonstrate any information necessary to identify the
25 consumer is kept separately and is subject to effective technical and
26 organizational controls that prevent the controller from accessing
27 such information.
28 (3) A controller that uses pseudonymous data or deidentified data
29 must exercise reasonable oversight to monitor compliance with any
30 contractual commitments to which the pseudonymous data or
31 deidentified data are subject and must take appropriate steps to
32 address any breaches of contractual commitments.

33 NEW SECTION. **Sec. 109.** DATA PROTECTION ASSESSMENTS. (1)
34 Controllers must conduct and document a data protection assessment of
35 each of the following processing activities involving personal data:
36 (a) The processing of personal data for purposes of targeted
37 advertising;
38 (b) The processing of personal data for the purposes of the sale
39 of personal data;

(c) The processing of personal data for purposes of profiling,
where such profiling presents a reasonably foreseeable risk of: (i)
Unfair or deceptive treatment of, or disparate impact on, consumers;
(ii) financial, physical, or reputational injury to consumers; (iii)
a physical or other intrusion upon the solitude or seclusion, or the
private affairs or concerns, of consumers, where such intrusion would
be offensive to a reasonable person; or (iv) other substantial injury
to consumers;
     (d) The processing of sensitive data; and
     (e) Any processing activities involving personal data that
present a heightened risk of harm to consumers.
     Such data protection assessments must take into account the type
of personal data to be processed by the controller, including the
extent to which the personal data are sensitive data, and the context
in which the personal data are to be processed.
     (2) Data protection assessments conducted under subsection (1) of
this section must identify and weigh the benefits that may flow
directly and indirectly from the processing to the controller,
consumer, other stakeholders, and the public against the potential
risks to the rights of the consumer associated with such processing,
as mitigated by safeguards that can be employed by the controller to
reduce such risks. The use of deidentified data and the reasonable
expectations of consumers, as well as the context of the processing
and the relationship between the controller and the consumer whose
personal data will be processed, must be factored into this
assessment by the controller.
     (3) The attorney general may request, in writing, that a
controller disclose any data protection assessment that is relevant
to an investigation conducted by the attorney general. The controller
must make a data protection assessment available to the attorney
general upon such a request. The attorney general may evaluate the
data protection assessments for compliance with the responsibilities
contained in section 107 of this act and, if it serves a civil
investigative demand, with RCW 19.86.110. Data protection assessments
are confidential and exempt from public inspection and copying under
chapter 42.56 RCW. The disclosure of a data protection assessment
pursuant to a request from the attorney general under this subsection
does not constitute a waiver of the attorney-client privilege or work
product protection with respect to the assessment and any information
contained in the assessment unless otherwise subject to case law

1 regarding the applicability of attorney-client privilege or work
2 product protections.

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

6 NEW SECTION. **Sec. 110.** LIMITATIONS AND APPLICABILITY. (1) The
7 obligations imposed on controllers or processors under this chapter
8 do not restrict a controller's or processor's ability to:
9 (a) Comply with federal, state, or local laws, rules, or
10 regulations;
11 (b) Comply with a civil, criminal, or regulatory inquiry,
12 investigation, subpoena, or summons by federal, state, local, or
13 other governmental authorities;
14 (c) Cooperate with law enforcement agencies concerning conduct or
15 activity that the controller or processor reasonably and in good
16 faith believes may violate federal, state, or local laws, rules, or
17 regulations;
18 (d) Investigate, establish, exercise, prepare for, or defend
19 legal claims;
20 (e) Provide a product or service specifically requested by a
21 consumer, perform a contract to which the consumer is a party, or
22 take steps at the request of the consumer prior to entering into a
23 contract;
24 (f) Take immediate steps to protect an interest that is essential
25 for the life of the consumer or of another natural person, and where
26 the processing cannot be manifestly based on another legal basis;
27 (g) Prevent, detect, protect against, or respond to security
28 incidents, identity theft, fraud, harassment, malicious or deceptive
29 activities, or any illegal activity; preserve the integrity or
30 security of systems; or investigate, report, or prosecute those
31 responsible for any such action;
32 (h) Engage in public or peer-reviewed scientific, historical, or
33 statistical research in the public interest that adheres to all other
34 applicable ethics and privacy laws and is approved, monitored, and
35 governed by an institutional review board, human subjects research
36 ethics review board, or a similar independent oversight entity that
37 determines: (i) If the research is likely to provide substantial
38 benefits that do not exclusively accrue to the controller; (ii) the
39 expected benefits of the research outweigh the privacy risks; and

1 (iii) if the controller has implemented reasonable safeguards to
2 mitigate privacy risks associated with research, including any risks
3 associated with reidentification; or
4   (i) Assist another controller, processor, or third party with any
5 of the obligations under this subsection.
6   (2) The obligations imposed on controllers or processors under
7 this chapter do not restrict a controller's or processor's ability to
8 collect, use, or retain data to:
9   (a) Identify and repair technical errors that impair existing or
10 intended functionality; or
11   (b) Perform solely internal operations that are reasonably
12 aligned with the expectations of the consumer based on the consumer's
13 existing relationship with the controller, or are otherwise
14 compatible with processing in furtherance of the provision of a
15 product or service specifically requested by a consumer or the
16 performance of a contract to which the consumer is a party when those
17 internal operations are performed during, and not following, the
18 consumer's relationship with the controller.
19   (3) The obligations imposed on controllers or processors under
20 this chapter do not apply where compliance by the controller or
21 processor with this chapter would violate an evidentiary privilege
22 under Washington law and do not prevent a controller or processor
23 from providing personal data concerning a consumer to a person
24 covered by an evidentiary privilege under Washington law as part of a
25 privileged communication.
26   (4) A controller or processor that discloses personal data to a
27 third-party controller or processor in compliance with the
28 requirements of this chapter is not in violation of this chapter if
29 the recipient processes such personal data in violation of this
30 chapter, provided that, at the time of disclosing the personal data,
31 the disclosing controller or processor did not have actual knowledge
32 that the recipient intended to commit a violation. A third-party
33 controller or processor receiving personal data from a controller or
34 processor in compliance with the requirements of this chapter is
35 likewise not in violation of this chapter for the obligations of the
36 controller or processor from which it receives such personal data.
37   (5) Obligations imposed on controllers and processors under this
38 chapter shall not:

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

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

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

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

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

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

NEW SECTION. **Sec. 111.** PRIVATE RIGHT OF ACTION. (1) Except as provided in subsection (2) of this section, nothing in this chapter creates an independent cause of action, except for the actions brought by the attorney general to enforce this chapter. Except as provided in subsection (2) of this section, no person, except for the attorney general, may enforce the rights and protections created by this chapter in any action. However, nothing in this chapter limits any other independent causes of action enjoyed by any person, including any constitutional, statutory, administrative, or common law rights or causes of action. The rights and protections in this chapter are not exclusive, and to the extent that a person has the rights and protections in this chapter because of another law other

than this chapter, the person continues to have those rights and
protections notwithstanding the existence of this chapter.

(2) A consumer alleging a violation of section 103 or 107 (6),
(8), or (9) of this act may bring a civil action in any court of
competent jurisdiction. Remedies shall be limited to appropriate
injunctive relief. The court shall also award reasonable attorneys'
fees and costs to any prevailing plaintiff.

NEW SECTION. **Sec. 112.** ENFORCEMENT. (1) Except as provided in
section 111 of this act, chapter may be enforced solely by the
attorney general under the consumer protection act, chapter 19.86
RCW.

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

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

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

(5) Beginning July 31, 2023, in determining a civil penalty under
this chapter, the court must consider, as mitigating factors, a
controller's or processor's good faith efforts to comply with the
requirements of this chapter and any actions to cure or remedy the
violations before an action is filed.

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

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

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

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

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

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

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

5   NEW SECTION. **Sec. 117.** A new section is added to chapter 42.56
6   RCW to read as follows:
7   Data protection assessments submitted by a controller to the
8   attorney general in accordance with requirements under section 109 of
9   this act are exempt from disclosure under this chapter.

10   NEW SECTION. **Sec. 118.** A new section is added to chapter 44.28
11   RCW to read as follows:
12   (1) By December 1, 2023, the joint committee must review the
13   efficacy of the attorney general providing controllers and processors
14   with warning letters and 30 days to cure alleged violations in the
15   warning letters pursuant to section 112 of this act and report its
16   findings to the governor and the appropriate committees of the
17   legislature.
18   (2) The report must include, but not be limited to:
19   (a) The number of warning letters the attorney general sent to
20   controllers and processors;
21   (b) A list of the controller and processor names that received
22   the warning letters;
23   (c) The categories of violations and the number of violations per
24   category;
25   (d) The number of actions brought by the attorney general as
26   authorized in this act due to a controller or processor not curing
27   the alleged violations within 30 days;
28   (e) The types of resources, including associated costs, expended
29   when providing warning letters and tracking compliance; and
30   (f) A recommendation on whether the warning letters provided by
31   the attorney general should be continued.
32   (3) The office of the attorney general shall provide the joint
33   committee any data within their purview that the joint committee
34   considers necessary to conduct the review.
35   (4) This section expires June 30, 2024.

36   **PART 2**
37   **Data Privacy Regarding Public Health Emergency—Private Sector**

1   NEW SECTION. **Sec. 201.** The definitions in this section apply
2   throughout this chapter unless the context clearly requires
3   otherwise.
4   (1) "Authenticate" means to use reasonable means to determine
5   that a request to exercise any of the rights in section 203 of this
6   act is being made by the consumer who is entitled to exercise the
7   rights with respect to the covered data at issue.
8   (2) "Business associate" has the same meaning as in Title 45
9   C.F.R. Part 160, established pursuant to the federal health insurance
10   portability and accountability act of 1996.
11   (3) "Child" has the same meaning as defined in the children's
12   online privacy protection act, Title 15 U.S.C. Sec. 6501 through
13   6506.
14   (4) "Consent" means any freely given, specific, informed, and
15   unambiguous indication of the consumer's wishes by which the consumer
16   signifies agreement to the processing of personal data relating to
17   the consumer for a narrowly defined particular purpose. Acceptance of
18   a general or broad terms of use or similar document that contains
19   descriptions of personal data processing along with other, unrelated
20   information, does not constitute consent. Hovering over, muting,
21   pausing, or closing a given piece of content does not constitute
22   consent. Likewise, agreement obtained through dark patterns does not
23   constitute consent.
24   (5)(a) "Consumer" means a natural person who is a Washington
25   resident acting only in an individual or household context.
26   (b) "Consumer" does not include a natural person acting in a
27   commercial or employment context.
28   (6) "Controller" means the natural or legal person that, alone or
29   jointly with others, determines the purposes and means of the
30   processing of covered data.
31   (7) "Covered data" includes personal data and one or more of the
32   following: Specific geolocation data; proximity data; or personal
33   health data.
34   (8) "Covered entity" has the same meaning as defined in Title 45
35   C.F.R. Part 160, established pursuant to the federal health insurance
36   portability and accountability act of 1996.
37   (9) "Covered purpose" means processing of covered data concerning
38   a consumer for the purposes of detecting symptoms of an infectious
39   disease, enabling the tracking of a consumer's contacts with other
40   consumers, or with specific locations to identify in an automated

fashion whom consumers have come into contact with, or digitally
notifying, in an automated manner, a consumer who may have become
exposed to an infectious disease, or other similar purposes directly
related to a state of emergency declared by the governor pursuant to
RCW 43.06.010 and any restrictions imposed under the state of
emergency declared by the governor pursuant to RCW 43.06.200 through
43.06.270.

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

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

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

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

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

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

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

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

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

(19) "Process," "processed," or "processing" means any operation
or set of operations that are performed on covered data or on sets of

covered data by automated means, such as the collection, use,
storage, disclosure, analysis, deletion, or modification of covered
data.

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

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

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

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

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

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

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

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

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

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

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

(b) The consumer provides consent for the processing;

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

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

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

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

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

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

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

17   NEW SECTION. **Sec. 204.** EXERCISING CONSUMER RIGHTS. (1) A
18 consumer may exercise the rights set forth in section 203 of this act
19 by submitting a request, at any time, to a controller specifying
20 which rights the consumer wishes to exercise.

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

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

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

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

1   (b) Controllers may not require a consumer to create a new
2 account in order to exercise a right, but a controller may require a
3 consumer to use an existing account to exercise the consumer's rights
4 under this chapter.
5   (3) A controller must comply with a request to exercise the right
6 in section 203(1) of this act as soon as feasibly possible, but no
7 later than 15 days of receipt of the request.
8   (4)(a) A controller must inform a consumer of any action taken on
9 a request to exercise any of the rights in section 203 (2) through
10 (4) of this act without undue delay and in any event within 45 days
11 of receipt of the request. That period may be extended once by 45
12 additional days where reasonably necessary, taking into account the
13 complexity and number of the requests. The controller must inform the
14 consumer of any such extension within 45 days of receipt of the
15 request, together with the reasons for the delay.
16   (b) If a controller does not take action on the request of a
17 consumer, the controller must inform the consumer without undue delay
18 and within 45 days of receipt of the request, of the reasons for not
19 taking action and instructions for how to appeal the decision with
20 the controller as described in subsection (5) of this section.
21   (c) Information provided under this section must be provided by
22 the controller to the consumer free of charge, up to twice annually.
23 Where requests from a consumer are manifestly unfounded or excessive,
24 because of their repetitive character, the controller may either: (i)
25 Charge a reasonable fee to cover the administrative costs of
26 complying with the request; or (ii) refuse to act on the request. The
27 controller bears the burden of demonstrating the manifestly unfounded
28 or excessive character of the request.
29   (d) A controller is not required to comply with a request to
30 exercise any of the rights under section 203 (1) through (4) of this
31 act if the controller is unable to authenticate the request using
32 commercially reasonable efforts. In such a case, the controller may
33 request the provision of additional information reasonably necessary
34 to authenticate the request.
35   (5)(a) Controllers must establish an internal process whereby
36 consumers may appeal a refusal to take action on a request to
37 exercise any of the rights under section 203 of this act within a
38 reasonable period of time after the consumer's receipt of the notice
39 sent by the controller under subsection (4)(b) of this section.

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

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

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

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

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

33   (a) Taking into account the nature of the processing, the
34 processor shall assist the controller by appropriate technical and
35 organizational measures, insofar as this is possible, for the
36 fulfillment of the controller's obligation to respond to consumer
37 requests to exercise their rights pursuant to section 203 of this
38 act; and

1   (b) Taking into account the nature of processing and the
2 information available to the processor, the processor shall assist
3 the controller in meeting the controller's obligations in relation to
4 the security of processing the personal data and in relation to the
5 notification of a breach of the security of the system pursuant to
6 RCW 19.255.010.
7   (3) Notwithstanding the instructions of the controller, a
8 processor shall:
9   (a) Ensure that each person processing the personal data is
10 subject to a duty of confidentiality with respect to the data; and
11   (b) Engage a subcontractor only after providing the controller
12 with an opportunity to object and pursuant to a written contract in
13 accordance with subsection (5) of this section that requires the
14 subcontractor to meet the obligations of the processor with respect
15 to the personal data.
16   (4) Taking into account the context of processing, the controller
17 and the processor shall implement appropriate technical and
18 organizational measures to ensure a level of security appropriate to
19 the risk and establish a clear allocation of the responsibilities
20 between them to implement such measures.
21   (5) Processing by a processor must be governed by a contract
22 between the controller and the processor that is binding on both
23 parties and that sets out the processing instructions to which the
24 processor is bound, including the nature and purpose of the
25 processing, the type of personal data subject to the processing, the
26 duration of the processing, and the obligations and rights of both
27 parties. In addition, the contract must include the requirements
28 imposed by this subsection and subsections (3) and (4) of this
29 section, as well as the following requirements:
30   (a) At the choice of the controller, the processor shall delete
31 or return all personal data to the controller as requested at the end
32 of the provision of services, unless retention of the personal data
33 is required by law;
34   (b)(i) The processor shall make available to the controller all
35 information necessary to demonstrate compliance with the obligations
36 in this chapter; and
37   (ii) The processor shall allow for, and contribute to, reasonable
38 audits and inspections by the controller or the controller's
39 designated auditor. Alternatively, the processor may, with the
40 controller's consent, arrange for a qualified and independent auditor

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

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

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

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

26   (a) How a consumer may exercise the rights contained in section
27 203 of this act, including how a consumer may appeal a controller's
28 action with regard to the consumer's request;

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

30   (c) The purposes for which the categories of covered data are
31 processed;

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

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

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

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

4   (4) Except as provided in this chapter, a controller may not
5 process covered data for purposes that are not reasonably necessary
6 to, or compatible with, the covered purposes for which the personal
7 data is processed unless the controller obtains the consumer's
8 consent. Controllers may not process covered data or deidentified
9 data that was processed for a covered purpose for purposes of
10 marketing, developing new products or services, or engaging in
11 commercial product or market research.

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

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

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

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

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

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

38   (b) Process deidentified information to engage in public or peer-
39 reviewed scientific, historical, or statistical research in the

public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that determines: (i) If the research is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) the expected benefits of the research outweigh the privacy risks; and (iii) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

(2) This chapter does not apply to:

(a) Information that meets the definition of:

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

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

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

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

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

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

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

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

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

(d) Data maintained for employment records purposes.

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

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

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

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

NEW SECTION. **Sec. 209.** PRIVATE RIGHT OF ACTION. (1) Except as provided in subsection (2) of this section, nothing in this chapter creates an independent cause of action, except for the actions brought by the attorney general to enforce this chapter. Except as provided in subsection (2) of this section, no person, except for the attorney general, may enforce the rights and protections created by this chapter in any action. However, nothing in this chapter limits any other causes of action enjoyed by any person, including any constitutional, statutory, administrative, or common law rights or causes of action. The rights and protections in this chapter are not exclusive, and to the extent that a person has the rights and protections in this chapter because of another law other than this chapter, the person continues to have those rights and protections notwithstanding the existence of this chapter.

(2) A consumer alleging a violation of section 203 or 207(7) of this act may bring a civil action in any court of competent jurisdiction. Remedies shall be limited to appropriate injunctive relief. The court shall also award reasonable attorneys' fees and costs to any prevailing plaintiff.

NEW SECTION. **Sec. 210.** ENFORCEMENT. (1) Except as provided in section 209 of this act, this chapter may be enforced solely by the attorney general under the consumer protection act, chapter 19.86 RCW.

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

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

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

(5) Beginning July 31, 2023, in determining a civil penalty under this chapter, the court must consider, as mitigating factors, a controller's or processor's good faith efforts to comply with the requirements of this chapter and any actions to cure or remedy the violations before an action is filed.

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

1　　NEW SECTION.　**Sec. 211.**　PREEMPTION. (1) Except as provided in
2　this section, this chapter supersedes and preempts laws, ordinances,
3　regulations, or the equivalent adopted by any local entity regarding
4　the processing of covered data for a covered purpose by controllers
5　or processors.
6　　　(2) Laws, ordinances, or regulations regarding the processing of
7　covered data for a covered purpose by controllers or processors that
8　are adopted by any local entity prior to July 1, 2020, are not
9　superseded or preempted.

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

14　　　　　　　　　　　　　　　　**PART 3**
15　　　**Data Privacy Regarding Public Health Emergency—Public Sector**

16　　NEW SECTION.　**Sec. 301.**　The definitions in this section apply
17　throughout this chapter unless the context clearly requires
18　otherwise.
19　　　(1) "Consent" means any freely given, specific, informed, and
20　unambiguous indication of the consumer's wishes by which the consumer
21　signifies agreement to the processing of personal data relating to
22　the consumer for a narrowly defined particular purpose. Acceptance of
23　a general or broad terms of use or similar document that contains
24　descriptions of personal data processing along with other, unrelated
25　information, does not constitute consent. Hovering over, muting,
26　pausing, or closing a given piece of content does not constitute
27　consent. Likewise, agreement obtained through dark patterns does not
28　constitute consent.
29　　　(2) "Controller" means the local government, state agency, or
30　institutions of higher education that, alone or jointly with others,
31　determines the purposes and means of the processing of technology-
32　assisted contact tracing information.
33　　　(3)(a) "Deidentified data" means data that cannot reasonably be
34　used to infer information about, or otherwise be linked to, an
35　identified or identifiable natural person, or a device linked to such
36　a person, provided that the controller that possesses the data: (i)
37　Takes reasonable measures to ensure that the data cannot be

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) The individual provides consent for the processing;

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

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

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

1   NEW SECTION. **Sec. 303.** RESPONSIBILITY ACCORDING TO ROLE. (1)
2   Controllers and processors are responsible for meeting their
3   respective obligations established under this chapter.
4   (2) Processors are responsible under this chapter for adhering to
5   the instructions of the controller and assisting the controller to
6   meet its obligations under this chapter. This assistance must include
7   the processor assisting the controller in meeting the controller's
8   obligations in relation to the security of processing technology-
9   assisted contact tracing information and in relation to the
10   notification of a breach of the security of the system pursuant to
11   RCW 42.56.590.
12   (3) Notwithstanding the instructions of the controller, a
13   processor shall:
14   (a) Ensure that each person processing the technology-assisted
15   contact tracing information is subject to a duty of confidentiality
16   with respect to the information; and
17   (b) Engage a subcontractor only after providing the controller
18   with an opportunity to object and pursuant to a written contract in
19   accordance with subsection (5) of this section that requires the
20   subcontractor to meet the obligations of the processor with respect
21   to the technology-assisted contact tracing information.
22   (4) Taking into account the context of processing, the controller
23   and the processor shall implement appropriate technical and
24   organizational measures to ensure a level of security appropriate to
25   the risk and establish a clear allocation of the responsibilities
26   between them to implement such measures.
27   (5) Processing by a processor must be governed by a contract or
28   data-sharing agreement between the controller and the processor that
29   is binding on both parties and that sets out the processing
30   instructions to which the processor is bound, including the nature
31   and purpose of the processing, the type of data subject to the
32   processing, the duration of the processing, and the obligations and
33   rights of both parties. In addition, the contract or data-sharing
34   agreement must include the requirements imposed by this subsection
35   and subsections (3) and (4) of this section, as well as the following
36   requirements:
37   (a) At the choice of the controller, the processor shall delete
38   or return all technology-assisted contact tracing information to the
39   controller as requested at the end of the provision of services,

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

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

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

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

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

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

1   (a) The categories of technology-assisted contact tracing
2 information processed by the controller;
3   (b) The purposes for which the categories of technology-assisted
4 contact tracing information are processed;
5   (c) The categories of technology-assisted contact tracing
6 information that the controller shares with third parties, if any;
7 and
8   (d) The categories of third parties, if any, with whom the
9 controller shares technology-assisted contact tracing information.
10   (2) A controller's collection of technology-assisted contact
11 tracing information must be limited to what is reasonably necessary
12 in relation to the technology-assisted contact tracing purpose for
13 which the information is processed.
14   (3) A controller's collection of technology-assisted contact
15 tracing information must be adequate, relevant, and limited to what
16 is reasonably necessary in relation to the technology-assisted
17 contact tracing purposes for which the information is processed.
18   (4) Except as provided in this chapter, a controller may not
19 process technology-assisted contact tracing information for purposes
20 that are not reasonably necessary to, or compatible with, the
21 technology-assisted contact tracing purposes for which the
22 technology-assisted contact tracing information is processed unless
23 the controller obtains the individual's consent. Controllers may not
24 process technology-assisted contact tracing information or
25 deidentified data that was processed for a technology-assisted
26 contact tracing purpose for purposes of marketing, developing new
27 products or services, or engaging in commercial product or market
28 research.
29   (5) A controller shall establish, implement, and maintain
30 reasonable administrative, technical, and physical data security
31 practices to protect the confidentiality, integrity, and
32 accessibility of technology-assisted contact tracing information.
33 These data security practices must be appropriate to the volume and
34 nature of the data at issue.
35   (6) A controller must delete or deidentify all technology-
36 assisted contact tracing information when the information is no
37 longer being used for a technology-assisted contact tracing purpose
38 and has met records retention as required by federal or state law.
39   (7) A controller may not process technology-assisted contact
40 tracing information on the basis of an individual's or a class of

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

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

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

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

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

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

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

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

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

18   NEW SECTION. **Sec. 307.** ENFORCEMENT. (1) Any waiver of the
19 provisions of this chapter is contrary to public policy and is void
20 and unenforceable.
21   (2)(a) Any individual injured by a violation of this chapter may
22 institute a civil action to recover damages.
23   (b) Any controller that violates, proposes to violate, or has
24 violated this chapter may be enjoined.
25   (c) The rights and remedies available under this chapter are
26 cumulative to each other and to any other rights and remedies
27 available under law.

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

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

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

1   <u>NEW SECTION.</u> **Sec. 401.** (1) Sections 101 through 114 of this act
2   constitute a new chapter in Title 19 RCW.
3   (2) Sections 201 through 211 of this act constitute a new chapter
4   in Title 19 RCW.
5   (3) Sections 301 through 308 of this act constitute a new chapter
6   in Title 43 RCW.

7   <u>NEW SECTION.</u> **Sec. 402.** Sections 1, 2, and 101 through 118 of
8   this act take effect July 31, 2022.

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

12   <u>NEW SECTION.</u> **Sec. 404.** Except for sections 1, 2, and 101
13   through 118 of this act, this act is necessary for the immediate
14   preservation of the public peace, health, or safety, or support of
15   the state government and its existing public institutions, and takes
16   effect immediately."

17   Correct the title.

       <u>EFFECT:</u> Makes the following changes in Part I of the bill
relating to consumer personal data privacy:
       (1) Modifies the definition of "deidentified data" to require
that controllers take reasonable measures to ensure that the data
cannot be associated not only with a natural person, but also with a
household or device.
       (2) Specifies that personal data includes pseudonymous data.
       (3) Adds the definition of "minor" to mean an individual who is
at least 13 and under 16 years of age under circumstances where a
controller has actual knowledge of, or willfully disregards, the
minor's age.
       (4) Modifies the definition of "targeted advertising" to mean
displaying advertisements selected on the basis of a consumer's
activities across one or more distinctly branded websites, rather
than across nonaffiliated websites. Specifies that targeted
advertising does not include advertising based on activities within a
controller's own commonly branded websites, rather than a
controller's own websites.
       (5) Exempts from the bill nonprofit organizations that are
registered with the Secretary of State under the Charities Program,
collect personal data during legitimate activities related to the
organization's tax-exempt purpose, and do not sell personal data
collected by the organization.
       (6) Provides that a consumer has the right to access the personal
data a controller is processing, rather than the right to access the
categories of personal data a controller is processing.

(7) Provides that, beginning July 31, 2023, a consumer may exercise the right to opt out of sale and targeted advertising by designating an authorized agent or via user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicates or signals the consumer's choice to opt out.

(8) Provides that a controller must respond to a request to exercise the right to access personal data within 45 days of receiving the request.

(9) Allows a consumer to appeal within a reasonable period of time after a controller refuses to take action on the consumer's right request, rather than after the consumer's receipt of the controller's notice that the controller did not take action on the consumer's request.

(10) Requires the mandatory privacy notice to use clear and plain language and be understandable to the least sophisticated consumer, as well as be in English and any other language in which a controller communicates with the consumer to whom the information pertains.

(11) Requires controllers to obtain a minor's consent prior to processing the minor's personal data for the purposes of targeted advertising or the sale of personal data.

(12) Adds a private right of action for consumers alleging a violation of the consumer data rights. Limits remedies to appropriate injunctive relief and requires the court to award reasonable attorneys' fees and costs to any prevailing plaintiff.

(13) Expires the right to cure violations one year after the effective date of the bill. Removes the statutory penalties from the provisions related to enforcement by the Attorney General and instead provides that after the expiration of the right to cure, when determining a civil penalty, the court must consider a controller's or processor's good faith efforts to cure as mitigating factors.

(14) Provides that the bill does not create any independent causes of action, except for the actions brought by the Attorney General. Specifies that nothing in the bill limits any other causes of action and that the rights and protections in the bill are not exclusive.

(13) Requires the Joint Legislative Audit and Review Committee study on the efficacy of the Attorney General providing controllers and processors to be completed by December 1, 2023, rather than December 1, 2025.

Makes the following changes to Part 2 of the bill relating to data privacy and public health emergency (private sector):

(1) Modifies the definition of "consent" to align with the same definition in Part 1 of the bill relating to consumer personal data privacy.

(2) Modifies the definition of "deidentified data" to require that controllers take reasonable measures to ensure that the data cannot be associated not only with a natural person, but also with a household or device.

(3) Adds a private right of action for consumers alleging a violation of the consumer data rights. Limits remedies to appropriate injunctive relief and requires the court to award reasonable attorneys' fees and costs to any prevailing plaintiff.

(4) Expires the right to cure violations one year after the effective date of the bill. Removes the statutory penalties from the provisions related to enforcement by the Attorney General and instead provides that after the expiration of the right to cure, when determining a civil penalty, the court must consider a controller's or processor's good faith efforts to cure as mitigating factors.

(5) Provides that the bill does not create any independent causes of action, except for the actions brought by the Attorney General. Specifies that nothing in the bill limits any other causes of action and that the rights and protections in the bill are not exclusive.

Makes the following changes to Part 3 of the bill relating to data privacy and public health emergency (public sector):

(1) Modifies the definition of "consent" to align with the same definition in Part 1 of the bill relating to consumer personal data privacy.

(2) Modifies the definition of "deidentified data" to require that controllers take reasonable measures to ensure that the data cannot be associated not only with a natural person, but also with a household or device.

Makes nonsubstantive technical corrections, such as correcting "if" to "is" in the definition of "technology-assisted contact tracing" in Part 3 of the bill.

--- END ---