
SECOND SUBSTITUTE SENATE BILL 5376

State of Washington

66th Legislature

2019 Regular Session

By Senate Ways & Means (originally sponsored by Senators Carlyle, Palumbo, Wellman, Mullet, Pedersen, Billig, Hunt, Liias, Rolfes, Saldaña, Hasegawa, and Keiser)

READ FIRST TIME 03/01/19.

1 AN ACT Relating to the management and oversight of personal data;
2 amending RCW 43.105.369; adding a new section to chapter 9.73 RCW;
3 adding a new chapter to Title 19 RCW; creating new sections;
4 prescribing penalties; and providing an effective date.

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

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

8 NEW SECTION. **Sec. 2.** LEGISLATIVE FINDINGS. (1) The legislature
9 finds that:

10 (a) Washingtonians cherish privacy as an element of their
11 individual freedom.

12 (b) Washington is a technology leader on a national and global
13 level and recognizes its distinctive position in promoting the
14 efficient balance of consumer privacy and economic benefits.

15 (c) Washington explicitly recognizes its citizens' right to
16 privacy under Article I, section 7 of the state Constitution.

17 (d) There is rapid growth in the volume and variety of personal
18 data being generated, collected, stored, and analyzed. This growth
19 has the potential for great benefits to human knowledge,

1 technological innovation, and economic growth, but also the potential
2 to harm individual privacy and freedom.

3 (e) Millions of Washingtonians have been affected by electronic
4 data breaches and the resulting loss of privacy, and the net effect,
5 both financially and in the chilling of consumer confidence, has and
6 will continue to cost Washington state businesses.

7 (f) As technology and businesses continue to push the limits of
8 data collection with exponential rapidity, laws must keep pace as
9 technology and business practices evolve to protect businesses and
10 consumers.

11 (g) There is a need to preserve individuals' trust and confidence
12 that personal data will be protected appropriately, while supporting
13 flexibility and the free flow of information. Meeting this need will
14 promote continued innovation and economic growth in the networked
15 economy.

16 (h) Enforcement of general principles in law will ensure that
17 citizens continue to enjoy meaningful privacy protections while
18 affording ample flexibility for technologies and business models to
19 evolve.

20 (i) The European Union recently updated its privacy law through
21 the passage and implementation of the general data protection
22 regulation, affording its residents the strongest privacy protections
23 in the world. Washington residents deserve to enjoy the same level of
24 robust privacy safeguards.

25 (j) In addition, the technology industry has been a tremendous
26 driver of economic growth in Washington state. We need to ensure that
27 any new privacy laws not only provide Washington residents with
28 strong privacy protections but also enable industry and others to use
29 data to create innovative technologies, products, and solutions.

30 (k) Technology will continue to evolve and change. Consequently,
31 any new privacy laws must be technology neutral and flexible, so that
32 they may apply not only to the technologies and products of today,
33 but to the technologies and products of tomorrow.

34 (l) Washington residents have long enjoyed an expectation of
35 privacy in their public movements. The development of new technology
36 like facial recognition could, if deployed indiscriminately and
37 without guardrails, enable the constant surveillance of any
38 individual any time of the day and every day of the year. Washington
39 residents should have the right to a reasonable expectation of
40 privacy in their movements, and thus should be free from ubiquitous

1 and surreptitious surveillance using facial recognition technology.
2 Further, Washington residents should have the right to expect
3 information about the capabilities and limitations of facial
4 recognition technology and that it should not be deployed by private
5 sector organizations without proper public notice.

6 (2) As such, the legislature recognizes the consumer protection
7 principles in this act regarding transparency, individual control,
8 respect for context, focused collection and responsible use,
9 security, access, and accuracy.

10 NEW SECTION. **Sec. 3.** DEFINITIONS. The definitions in this
11 section apply throughout this chapter unless the context clearly
12 requires otherwise.

13 (1) "Affiliate" means a legal entity that controls, is controlled
14 by, or is under common control with, another legal entity.

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

18 (3) "Business purpose" means the processing of personal data for
19 the controller's or its processor's operational purposes, or other
20 notified purposes, provided that the processing of personal data must
21 be reasonably necessary and proportionate to achieve the operational
22 purposes for which the personal data was collected or processed or
23 for another operational purpose that is compatible with the context
24 in which the personal data was collected. Business purposes include:

25 (a) Auditing related to a current interaction with the consumer
26 and concurrent transactions including, but not limited to, counting
27 ad impressions, verifying positioning and quality of ad impressions,
28 and auditing compliance with this specification and other standards;

29 (b) Detecting security incidents, protecting against malicious,
30 deceptive, fraudulent, or illegal activity, and prosecuting those
31 responsible for that activity;

32 (c) Identifying and repairing errors that impair existing or
33 intended functionality;

34 (d) Short-term, transient use, provided the personal data is not
35 disclosed to another third party and is not used to build a profile
36 about a consumer or otherwise alter an individual consumer's
37 experience outside the current interaction including, but not limited
38 to, the contextual customization of ads shown as part of the same
39 interaction;

1 (e) Maintaining or servicing accounts, providing customer
2 service, processing or fulfilling orders and transactions, verifying
3 customer information, processing payments, or providing financing;

4 (f) Undertaking internal research for technological development;
5 or

6 (g) Authenticating a consumer's identity.

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

8 (5) "Consent" means a clear affirmative act signifying a
9 specific, informed, and unambiguous indication of a consumer's
10 agreement to the processing of personal data relating to the
11 consumer, such as by a written statement or other clear affirmative
12 action.

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

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

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

23 (9)(a) "Data broker" means a business, or unit or units of a
24 business, separately or together, that knowingly collects and sells
25 or licenses to third parties the brokered personal information of a
26 consumer with whom the business does not have a direct relationship.

27 (b) Providing publicly available information through real-time or
28 near real-time alert services for health or safety purposes, and the
29 collection and sale or licensing of brokered personal information
30 incidental to conducting those activities, does not qualify the
31 business as a data broker.

32 (c) The phrase "sells or licenses" does not include:

33 (i) A one-time or occasional sale of assets that is not part of
34 the ordinary conduct of the business;

35 (ii) A sale or license of data that is merely incidental to the
36 business; or

37 (iii) Providing 411 directory assistance or directory information
38 services, including name, address, and telephone number, on behalf of
39 or as a function of a telecommunications carrier.

40 (10) "Deidentified data" means:

1 (a) Data that cannot be linked to a known natural person without
2 additional information kept separately; or

3 (b) Data (i) that has been modified to a degree that the risk of
4 reidentification is small, (ii) that is subject to a public
5 commitment by the controller not to attempt to reidentify the data,
6 and (iii) to which one or more enforceable controls to prevent
7 reidentification has been applied. Enforceable controls to prevent
8 reidentification may include legal, administrative, technical, or
9 contractual controls.

10 (11) "Developer" means a person who creates or modifies the set
11 of instructions or programs instructing a computer or device to
12 perform tasks.

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

15 (13) "Health care information" has the same meaning as in RCW
16 70.02.010.

17 (14) "Health care provider" has the same meaning as in RCW
18 70.02.010.

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

21 (16) "Personal data" means any information that is linked or
22 reasonably linkable to an identified or identifiable natural person.
23 Personal data does not include deidentified data or publicly
24 available information. For these purposes, "publicly available
25 information" means information that is lawfully made available from
26 federal, state, or local government records.

27 (17) "Process" or "processing" means any collection, use,
28 storage, disclosure, analysis, deletion, or modification of personal
29 data.

30 (18) "Processor" means a natural or legal person that processes
31 personal data on behalf of the controller.

32 (19) "Profiling" means any form of automated processing of
33 personal data consisting of the use of personal data to evaluate
34 certain personal aspects relating to a natural person, in particular
35 to analyze or predict aspects concerning that natural person's
36 economic situation, health, personal preferences, interests,
37 reliability, behavior, location, or movements.

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

1 (21) "Restriction of processing" means the marking of stored
2 personal data with the aim of limiting the processing of such
3 personal data in the future.

4 (22)(a) "Sale," "sell," or "sold" means the exchange of personal
5 data for monetary consideration by the controller to a third party
6 for purposes of licensing or selling personal data at the third
7 party's discretion to additional third parties.

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

21 (23) "Sensitive data" means (a) personal data revealing racial or
22 ethnic origin, religious beliefs, mental or physical health condition
23 or diagnosis, or sex life or sexual orientation; (b) the processing
24 of genetic or biometric data for the purpose of uniquely identifying
25 a natural person; or (c) the personal data of a known child.

26 (24) "Targeted advertising" means displaying advertisements to a
27 consumer where the advertisement is selected based on personal data
28 obtained or inferred over time from a consumer's activities across
29 nonaffiliated web sites, applications, or online services to predict
30 user preferences or interests. It does not include advertising to a
31 consumer based upon the consumer's visits to a web site, application,
32 or online service that a reasonable consumer would believe to be
33 associated with the publisher where the ad is placed based on common
34 branding, trademarks, or other indicia of common ownership, or in
35 response to the consumer's request for information or feedback.

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

39 (26) "Verified request" means the process through which a
40 consumer may submit a request to exercise a right or rights set forth

1 in this chapter, and by which a controller can reasonably
2 authenticate the request and the consumer making the request using
3 commercially reasonable means.

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

9 (a) Controls or processes personal data of one hundred thousand
10 consumers or more; or

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

14 (2) This chapter does not apply to:

15 (a) State and local governments;

16 (b) Municipal corporations;

17 (c) Information that meets the definition of:

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

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

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

24 (iv) Identifiable private information for purposes of the federal
25 policy for the protection of human subjects, 45 C.F.R. Part 46, or
26 identifiable private information that is otherwise information
27 collected as part of human subjects research pursuant to the good
28 clinical practice guidelines issued by the international council for
29 harmonisation, or the protection of human subjects under 21 C.F.R.
30 Parts 50 and 56;

31 (v) Information and documents created specifically for, and
32 collected and maintained by:

33 (A) A quality improvement committee for purposes of RCW
34 43.70.510, 70.230.080, or 70.41.200;

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

36 (C) A quality assurance committee for purposes of RCW 74.42.640
37 or 18.20.390;

38 (D) A hospital, as defined in RCW 43.70.056, for reporting of
39 health care-associated infections for purposes of RCW 43.70.056, a

1 notification of an incident for purposes of RCW 70.56.040(5), or
2 reports regarding adverse events for purposes of RCW 70.56.020(2)(b);

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

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

8 (d) Information maintained in the same manner as information
9 under (c) of this subsection 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. 290 dd-2;

17 (e) Personal data provided to, from, or held by a consumer
18 reporting agency as defined by 15 U.S.C. Sec. 1681a(f), and use of
19 that data is in compliance with the federal fair credit reporting act
20 (15 U.S.C. Sec. 1681 et seq.);

21 (f) Personal data collected, processed, sold, or disclosed
22 pursuant to the federal Gramm Leach Bliley act (P.L. 106-102), and
23 implementing regulations, if the collection, processing, sale, or
24 disclosure is in compliance with that law;

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

29 (h) Data maintained for employment records purposes.

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

31 Controllers are responsible for meeting the obligations established
32 under this chapter.

33 (2) Processors are responsible under this act for adhering to the
34 instructions of the controller and assisting the controller to meet
35 its obligations under this chapter.

36 (3) Processing by a processor is governed by a contract between
37 the controller and the processor that is binding on the processor and
38 that sets out the processing instructions to which the processor is
39 bound.

1 NEW SECTION.

Sec. 6.

CONSUMER RIGHTS. Controllers shall

2 facilitate verified requests to exercise the consumer rights set
3 forth in subsections (1) through (6) of this section.

4 (1) Upon a verified request from a consumer, a controller must
5 confirm whether or not personal data concerning the consumer is being
6 processed by the controller, including whether such personal data is
7 sold to data brokers, and, where personal data concerning the
8 consumer is being processed by the controller, provide access to such
9 personal data that the controller maintains in identifiable form
10 concerning the consumer.

11 (a) Upon a verified request from a consumer, a controller must
12 provide a copy of the personal data that the controller maintains in
13 identifiable form undergoing processing. For any further copies
14 requested by the consumer, the controller may charge a reasonable fee
15 based on administrative costs. Where the consumer makes the request
16 by electronic means, and unless otherwise requested by the consumer,
17 the information must be provided in a commonly used electronic form.

18 (b) This subsection does not adversely affect the rights or
19 freedoms of others.

20 (2) Upon a verified request from a consumer, the controller,
21 without undue delay, must correct inaccurate personal data that the
22 controller maintains in identifiable form concerning the consumer.
23 Taking into account the business purposes of the processing, the
24 controller must complete incomplete personal data, including by means
25 of providing a supplementary statement where appropriate.

26 (3) (a) Upon a verified request from a consumer, a controller must
27 delete, without undue delay, the consumer's personal data that the
28 controller maintains in identifiable form if one of the following
29 grounds applies:

30 (i) The personal data is no longer necessary for a business
31 purpose, including the provision of a product or service to the
32 consumer;

33 (ii) For processing that requires consent under section 8(3) of
34 this act, the consumer withdraws consent to processing and there are
35 no business purposes for the processing;

36 (iii) The consumer objects to the processing pursuant to
37 subsection (6) of this section and (A) there are no business purposes
38 for processing the personal data for the controller, the consumer
39 whose personal data is being processed, or the public, for which the

1 processing is necessary; or (B) the processing is for targeted
2 advertising;

3 (iv) The personal data has been unlawfully processed; or

4 (v) The personal data must be deleted to comply with a legal
5 obligation under federal, state, or local law to which the controller
6 is subject.

7 (b) Where the controller is obliged to delete personal data that
8 the controller maintains in identifiable form under this section that
9 has been disclosed to third parties by the controller, including data
10 brokers that received the personal data through a sale, the
11 controller must take reasonable steps, which may include technical
12 measures, to inform other controllers of which it is aware that are
13 processing such personal data, and that received such personal data
14 from the controller or are processing such personal data on behalf of
15 the controller, that the consumer has requested the deletion by the
16 other controllers of any links to, or copy or replication of, the
17 personal data. Compliance with this obligation must take into account
18 available technology and cost of implementation.

19 (c) This subsection does not apply to the extent processing is
20 necessary:

21 (i) For exercising the right of free speech;

22 (ii) For compliance with a legal obligation that requires
23 processing of personal data by federal, state, or local law, or
24 regulation to which the controller is subject or for the performance
25 of a task carried out in the public interest or in the exercise of
26 official authority vested in the controller;

27 (iii) For reasons of public interest in the area of public
28 health, where the processing (A) is subject to suitable and specific
29 measures to safeguard the rights of the consumer; and (B) is under
30 the responsibility of a professional subject to confidentiality
31 obligations under federal, state, or local law;

32 (iv) For archiving purposes in the public interest, scientific or
33 historical research purposes, or statistical purposes, where the
34 deletion of such personal data is likely to render impossible or
35 seriously impair the achievement of the objectives of the processing;

36 (v) For the establishment, exercise, or defense of legal claims;

37 (vi) To detect or respond to security incidents, protect against
38 malicious, deceptive, fraudulent, or illegal activity, or identify,
39 investigate, or prosecute those responsible for that activity; or

1 (vii) For a data broker that received the personal data from
2 third parties and is acting as a controller, solely to prevent the
3 personal data from reappearing in the future, in which case the
4 controller shall instead comply with the requirements in subsection
5 (4) of this section.

6 (4)(a) Upon a verified request from a consumer, the controller
7 must restrict processing of personal data that the controller
8 maintains in identifiable form if the purpose for which the personal
9 data is (i) not consistent with a purpose for which the personal data
10 was collected; (ii) not consistent with a purpose disclosed to the
11 consumer at the time of collection or authorization; or (iii)
12 unlawful.

13 (b) Where personal data is subject to a restriction of processing
14 under this subsection, the personal data must, with the exception of
15 storage, only be processed (i) with the consumer's consent; (ii) for
16 the establishment, exercise, or defense of legal claims; (iii) for
17 the protection of the rights of another natural or legal person; (iv)
18 for reasons of important public interest under federal, state, or
19 local law; (v) to provide products or services requested by the
20 consumer; or (vi) for another purpose set forth in subsection (3)(c)
21 of this section.

22 (c) A consumer who has obtained restriction of processing
23 pursuant to this subsection must be informed by the controller before
24 the restriction of processing is lifted.

25 (5)(a) Upon a verified request from a consumer, the controller
26 must provide to the consumer, if technically feasible and
27 commercially reasonable, any personal data that the controller
28 maintains in identifiable form concerning the consumer that such
29 consumer has provided to the controller in a structured, commonly
30 used, and machine-readable format if (i)(A) the processing of such
31 personal data requires consent under section 8(3) of this act, (B)
32 the processing of such personal data is necessary for the performance
33 of a contract to which the consumer is a party, or (C) in order to
34 take steps at the request of the consumer prior to entering into a
35 contract; and (ii) the processing is carried out by automated means.

36 (b) Requests for personal data under this subsection must be
37 without prejudice to the other rights granted in this chapter.

38 (c) The rights provided in this subsection do not apply to
39 processing necessary for the performance of a task carried out in the

1 public interest or in the exercise of official authority vested in
2 the controller, and must not adversely affect the rights of others.

3 (6) (a) A consumer may object through a verified request, on
4 grounds relating to the consumer's particular situation, at any time
5 to processing of personal data concerning such consumer.

6 (b) When a consumer objects to the processing of their personal
7 data for targeted advertising, which includes the sale of personal
8 data concerning the consumer to third parties for purposes of
9 targeted advertising, the controller must no longer process the
10 personal data subject to the objection for such purpose and must take
11 reasonable steps to communicate the consumer's objection, unless it
12 proves impossible or involves disproportionate effort, regarding any
13 further processing of the consumer's personal data for such purposes
14 to any third parties to whom the controller sold the consumer's
15 personal data for such purposes. Third parties must honor objection
16 requests pursuant to this subsection received from third-party
17 controllers.

18 (c) If a consumer objects to processing for any purposes, other
19 than targeted advertising, the controller may continue processing the
20 personal data subject to the objection if the controller can
21 demonstrate a legitimate ground to process such personal data that
22 overrides the potential risks to the rights of the consumer
23 associated with the processing, or if another exemption in this
24 chapter applies.

25 (7) A controller must communicate any correction, deletion, or
26 restriction of processing carried out in accordance with subsections
27 (2), (3), or (4) of this section to each third-party recipient to
28 whom the controller knows the personal data has been disclosed,
29 including third parties that received the data through a sale, within
30 one year preceding the verified request unless this proves
31 functionally impractical, technically infeasible, or involves
32 disproportionate effort, or the controller knows or is informed by
33 the third party that the third party is not continuing to use the
34 personal data. The controller must inform the consumer about third-
35 party recipients or categories with whom the controller shares
36 personal information, if any, if the consumer requests such
37 information.

38 (8) A controller must provide information on action taken on a
39 verified request under subsections (1) through (6) of this section
40 without undue delay and in any event within thirty days of receipt of

1 the request. That period may be extended by sixty additional days
2 where reasonably necessary, taking into account the complexity and
3 number of the requests. The controller must inform the consumer of
4 any such extension within thirty days of receipt of the request,
5 together with the reasons for the delay. Where the consumer makes the
6 request by electronic means, the information must be provided by
7 electronic means where possible, unless otherwise requested by the
8 consumer.

9 (a) If a controller does not take action on the request of a
10 consumer, the controller must inform the consumer without undue delay
11 and at the latest within thirty days of receipt of the request of the
12 reasons for not taking action and any possibility for internal review
13 of the decision by the controller.

14 (b) Information provided under this section must be provided by
15 the controller free of charge to the consumer. Where requests from a
16 consumer are manifestly unfounded or excessive, in particular because
17 of their repetitive character, the controller may either: (i) Charge
18 a reasonable fee taking into account the administrative costs of
19 providing the information or communication or taking the action
20 requested; or (ii) refuse to act on the request. The controller bears
21 the burden of demonstrating the manifestly unfounded or excessive
22 character of the request.

23 (c) Where the controller has reasonable doubts concerning the
24 identity of the consumer making a request under subsections (1)
25 through (6) of this section, the controller may request the provision
26 of additional information necessary to confirm the identity of the
27 consumer.

28 NEW SECTION. **Sec. 7.** TRANSPARENCY. (1) Controllers must be
29 transparent and accountable for their processing of personal data, by
30 making available in a form that is reasonably accessible to consumers
31 a clear, meaningful privacy notice that includes:

32 (a) The categories of personal data collected by the controller;

33 (b) The purposes for which the categories of personal data is
34 used and disclosed to third parties, if any;

35 (c) The rights that consumers may exercise pursuant to section 6
36 of this act, if any;

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

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

3 (2) If a controller sells personal data to data brokers or
4 processes personal data for targeted advertising, it must disclose
5 such processing, as well as the manner in which a consumer may
6 exercise the right to object to such processing, in a clear and
7 conspicuous manner.

8 NEW SECTION. **Sec. 8. RISK ASSESSMENTS.** (1) Controllers must
9 conduct, to the extent not previously conducted, a risk assessment of
10 each of their processing activities involving personal data and an
11 additional risk assessment any time there is a change in processing
12 that materially increases the risk to consumers. Such risk
13 assessments must take into account the type of personal data to be
14 processed by the controller, including the extent to which the
15 personal data is sensitive data or otherwise sensitive in nature, and
16 the context in which the personal data is to be processed.

17 (2) Risk assessments conducted under subsection (1) of this
18 section must identify and weigh the benefits that may flow directly
19 and indirectly from the processing to the controller, consumer, other
20 stakeholders, and the public, against the potential risks to the
21 rights of the consumer associated with such processing, as mitigated
22 by safeguards that can be employed by the controller to reduce such
23 risks. The use of deidentified data and the reasonable expectations
24 of consumers, as well as the context of the processing and the
25 relationship between the controller and the consumer whose personal
26 data will be processed, must factor into this assessment by the
27 controller.

28 (3) If the risk assessment conducted under subsection (1) of this
29 section determines that the potential risks of privacy harm to
30 consumers are substantial and outweigh the interests of the
31 controller, consumer, other stakeholders, and the public in
32 processing the personal data of the consumer, the controller may only
33 engage in such processing with the consent of the consumer or if
34 another exemption under this chapter applies. To the extent the
35 controller seeks consumer consent for processing, such consent shall
36 be as easy to withdraw as to give.

37 (4) Processing for a business purpose shall be presumed to be
38 permissible unless: (a) It involves the processing of sensitive data;

1 and (b) the risk of processing cannot be reduced through the use of
2 appropriate administrative and technical safeguards.

3 (5) The controller must make the risk assessment available to the
4 attorney general upon request. Risk assessments are confidential and
5 exempt from public inspection and copying under chapter 42.56 RCW.

6 NEW SECTION. **Sec. 9.** DEIDENTIFIED DATA. A controller or
7 processor that uses deidentified data must exercise reasonable
8 oversight to monitor compliance with any contractual commitments to
9 which the deidentified data is subject, and must take appropriate
10 steps to address any breaches of contractual commitments.

11 NEW SECTION. **Sec. 10.** EXEMPTIONS. (1) The obligations imposed
12 on controllers or processors under this chapter do not restrict a
13 controller's or processor's ability to:

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

16 (b) Comply with a civil, criminal, or regulatory inquiry,
17 investigation, subpoena, or summons by federal, state, local, or
18 other governmental authorities;

19 (c) Cooperate with law enforcement agencies concerning conduct or
20 activity that the controller or processor reasonably and in good
21 faith believes may violate federal, state, or local law;

22 (d) Investigate, exercise, or defend legal claims;

23 (e) Prevent or detect identity theft, fraud, or other criminal
24 activity or verify identities;

25 (f) Perform a contract to which the consumer is a party or in
26 order to take steps at the request of the consumer prior to entering
27 into a contract;

28 (g) Protect the vital interests of the consumer or of another
29 natural person;

30 (h) Perform a task carried out in the public interest or in the
31 exercise of official authority vested in the controller;

32 (i) Process personal data of a consumer for one or more specific
33 purposes where the consumer has given their consent to the
34 processing; or

35 (j) Prevent, detect, or respond to security incidents, identity
36 theft, fraud, harassment, malicious or deceptive activities, or any
37 illegal activity; preserve the integrity or security of systems; or

1 investigate, report, or prosecute those responsible for any such
2 action.

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

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

22 (4) This chapter does not require a controller or processor to do
23 the following:

24 (a) Reidentify deidentified data;

25 (b) Retain, link, or combine personal data concerning a consumer
26 that it would not otherwise retain, link, or combine in the ordinary
27 course of business;

28 (c) Comply with a request to exercise any of the rights under
29 section 6 (1) through (6) of this act if the controller is unable to
30 verify, using commercially reasonable efforts, the identity of the
31 consumer making the request.

32 (5) Obligations imposed on controllers and processors under this
33 chapter do not:

34 (a) Adversely affect the rights or freedoms of any persons; or

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

37 NEW SECTION. **Sec. 11.** LIABILITY. (1) This chapter does not
38 serve as the basis for a private right of action under this chapter
39 or any other law.

1 (2) Where more than one controller or processor, or both a
2 controller and a processor, involved in the same processing, is in
3 violation of this chapter, the liability shall be allocated among the
4 parties according to principles of comparative fault, unless such
5 liability is otherwise allocated by contract among the parties.

6 NEW SECTION. **Sec. 12.** ENFORCEMENT. (1) The legislature finds
7 that the practices covered by this chapter are matters vitally
8 affecting the public interest for the purpose of applying the
9 consumer protection act, chapter 19.86 RCW. A violation of this
10 chapter is not reasonable in relation to the development and
11 preservation of business and is an unfair or deceptive act in trade
12 or commerce and an unfair method of competition for the purpose of
13 applying the consumer protection act, chapter 19.86 RCW.

14 (2) The attorney general may bring an action in the name of the
15 state, or as *parens patriae* on behalf of persons residing in the
16 state, to enforce this chapter.

17 (3) A controller or processor is in violation of this chapter if
18 it fails to cure any alleged violation of sections 6 through 10 of
19 this act within thirty days after receiving notice of alleged
20 noncompliance. Any controller or processor that violates this chapter
21 is subject to an injunction and liable for a civil penalty of not
22 more than two thousand five hundred dollars for each violation or
23 seven thousand five hundred dollars for each intentional violation.

24 (4) The consumer privacy account is created in the state
25 treasury. All receipts from the imposition of civil penalties under
26 this chapter must be deposited into the account. Moneys in the
27 account may be spent only after appropriation. Expenditures from the
28 account may be used only to fund the office of privacy and data
29 protection as established under RCW 43.105.369.

30 NEW SECTION. **Sec. 13.** PREEMPTION. This chapter supersedes and
31 preempts laws, ordinances, regulations, or the equivalent adopted by
32 any local entity regarding the processing of personal data by
33 controllers or processors.

34 NEW SECTION. **Sec. 14.** FACIAL RECOGNITION. (1) Controllers using
35 facial recognition for profiling must employ meaningful human review
36 prior to making final decisions based on such profiling where such
37 final decisions produce legal effects concerning consumers or

1 similarly significant effects concerning consumers. Decisions
2 producing legal effects or similarly significant effects shall
3 include, but not be limited to, denial of consequential services or
4 support, such as financial and lending services, housing, insurance,
5 education enrollment, criminal justice, employment opportunities, and
6 health care services.

7 (2) Processors that provide facial recognition services must
8 provide documentation that includes general information that explains
9 the capabilities and limitations of the technology in terms that
10 customers and consumers can understand.

11 (3) Processors that provide facial recognition services must
12 prohibit, in the contract required by section 5 of this act, the use
13 of such facial recognition services by controllers to unlawfully
14 discriminate under federal or state law against individual consumers
15 or groups of consumers.

16 (4) Controllers must obtain consent from consumers prior to
17 deploying facial recognition services in physical premises open to
18 the public. The placement of conspicuous notice in physical premises
19 that clearly conveys that facial recognition services are being used
20 constitute a consumer's consent to the use of such facial recognition
21 services when that consumer enters those premises that have such
22 notice.

23 (5) Providers of commercial facial recognition services that make
24 their technology available as an online service for developers and
25 customers to use in their own scenarios must make available an
26 application programming interface or other technical capability,
27 chosen by the provider, to enable third parties that are legitimately
28 engaged in independent testing to conduct reasonable tests of those
29 facial recognition services for accuracy and unfair bias.

30 (6) For purposes of this section, "facial recognition" means
31 technology that analyzes facial features and is used for the unique
32 personal identification of natural persons in still or video images.

33 NEW SECTION. **Sec. 15.** A new section is added to chapter 9.73
34 RCW to read as follows:

35 (1) State and local government agencies shall not use facial
36 recognition technology to engage in ongoing surveillance of specified
37 individuals in public spaces, unless such use is in support of law
38 enforcement activities and either (a) a court order has been obtained
39 to permit the use of facial recognition services for that ongoing

1 surveillance; or (b) where there is an emergency involving imminent
2 danger or risk of death or serious physical injury to a person.

3 (2) This section applies to all Washington state and local
4 government agencies.

5 (3) For purposes of this section, "facial recognition" means the
6 same as in section 14 of this act.

7 **Sec. 16.** RCW 43.105.369 and 2016 c 195 s 2 are each amended to
8 read as follows:

9 (1) The office of privacy and data protection is created within
10 the office of the state chief information officer. The purpose of the
11 office of privacy and data protection is to serve as a central point
12 of contact for state agencies on policy matters involving data
13 privacy and data protection.

14 (2) The director shall appoint the chief privacy officer, who is
15 the director of the office of privacy and data protection.

16 (3) The primary duties of the office of privacy and data
17 protection with respect to state agencies are:

18 (a) To conduct an annual privacy review;

19 (b) To conduct an annual privacy training for state agencies and
20 employees;

21 (c) To articulate privacy principles and best practices;

22 (d) To coordinate data protection in cooperation with the agency;
23 and

24 (e) To participate with the office of the state chief information
25 officer in the review of major state agency projects involving
26 personally identifiable information.

27 (4) The office of privacy and data protection must serve as a
28 resource to local governments and the public on data privacy and
29 protection concerns by:

30 (a) Developing and promoting the dissemination of best practices
31 for the collection and storage of personally identifiable
32 information, including establishing and conducting a training program
33 or programs for local governments; and

34 (b) Educating consumers about the use of personally identifiable
35 information on mobile and digital networks and measures that can help
36 protect this information.

37 (5) By December 1, 2016, and every four years thereafter, the
38 office of privacy and data protection must prepare and submit to the
39 legislature a report evaluating its performance. The office of

1 privacy and data protection must establish performance measures in
2 its 2016 report to the legislature and, in each report thereafter,
3 demonstrate the extent to which performance results have been
4 achieved. These performance measures must include, but are not
5 limited to, the following:

6 (a) The number of state agencies and employees who have
7 participated in the annual privacy training;

8 (b) A report on the extent of the office of privacy and data
9 protection's coordination with international and national experts in
10 the fields of data privacy, data protection, and access equity;

11 (c) A report on the implementation of data protection measures by
12 state agencies attributable in whole or in part to the office of
13 privacy and data protection's coordination of efforts; and

14 (d) A report on consumer education efforts, including but not
15 limited to the number of consumers educated through public outreach
16 efforts, as indicated by how frequently educational documents were
17 accessed, the office of privacy and data protection's participation
18 in outreach events, and inquiries received back from consumers via
19 telephone or other media.

20 (6) Within one year of June 9, 2016, the office of privacy and
21 data protection must submit to the joint legislative audit and review
22 committee for review and comment the performance measures developed
23 under subsection (5) of this section and a data collection plan.

24 (7) The office of privacy and data protection shall submit a
25 report to the legislature on the: (a) Extent to which
26 telecommunications providers in the state are deploying advanced
27 telecommunications capability; and (b) existence of any inequality in
28 access to advanced telecommunications infrastructure experienced by
29 residents of tribal lands, rural areas, and economically distressed
30 communities. The report may be submitted at a time within the
31 discretion of the office of privacy and data protection, at least
32 once every four years, and only to the extent the office of privacy
33 and data protection is able to gather and present the information
34 within existing resources.

35 (8) The office of privacy and data protection must conduct an
36 analysis on the public sector use of facial recognition. By September
37 30, 2023, the office of privacy and data protection must submit a
38 report of its findings to the appropriate committees of the
39 legislature.

1 (9) The office of privacy and data protection, in consultation
2 with the attorney general, must by rule (a) establish any exceptions
3 to this chapter necessary to comply with state or federal law by the
4 effective date of this section and as necessary thereafter, (b)
5 clarify definitions of this chapter as necessary, and (c) create
6 exemption eligibility requirements for small businesses and research
7 institutions.

8 NEW SECTION. **Sec. 17.** Sections 3 through 14 of this act
9 constitute a new chapter in Title 19 RCW.

10 NEW SECTION. **Sec. 18.** This act takes effect July 31, 2021.

--- END ---