

---

**SENATE BILL 5377**

---

**State of Washington**

**66th Legislature**

**2019 Regular Session**

**By** Senators Carlyle, Palumbo, Mullet, Hasegawa, Keiser, and Pedersen

1 AN ACT Relating to data sales and governance; amending RCW  
2 43.105.020; adding new sections to chapter 43.105 RCW; creating new  
3 sections; and providing an effective date.

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

5 NEW SECTION. **Sec. 1.** This act may be known and cited as the  
6 data management and protection act.

7 NEW SECTION. **Sec. 2.** The legislature finds that:

8 (1) The Constitution and laws of the state of Washington provide  
9 for robust protection of personal privacy;

10 (2) Data breaches and internet crime have in recent years  
11 repeatedly compromised the safety and welfare of Washington residents  
12 and visitors;

13 (3) The people of the state expect and require their government  
14 to act as a good steward of all data with which it is entrusted;

15 (4) The public entrusts the state of Washington with their data  
16 and expects that it will be treated with a high degree of  
17 professionalism;

18 (5) The trust of the public is more valuable to the state than  
19 any funds to be derived from selling data;

1 (6) The legislature has only rarely deemed the sale of data to be  
2 in the public interest;

3 (7) The legislature created the office of privacy and data  
4 protection in part to enhance the practice of data stewardship among  
5 state agencies and local government;

6 (8) The people of the state expect state agencies to  
7 appropriately protect especially vulnerable people from unwarranted  
8 exposure, danger, or interference;

9 (9) The state's partners including businesses, governments, and  
10 other organizations are held to no lesser account than state agencies  
11 when conducting or supporting state functions;

12 (10) The state strives to make decisions based only on the best  
13 data available in order to ensure fairness and efficiency in the  
14 conduct of government; and

15 (11) Transparency and open data have been a priority for the  
16 legislature since the creation of the information access task force  
17 in 1995.

18 **Sec. 3.** RCW 43.105.020 and 2017 c 92 s 2 are each amended to  
19 read as follows:

20 The definitions in this section apply throughout this chapter  
21 unless the context clearly requires otherwise.

22 (1) "Agency" means the consolidated technology services agency.

23 (2) "Board" means the technology services board.

24 (3) "Customer agencies" means all entities that purchase or use  
25 information technology resources, telecommunications, or services  
26 from the consolidated technology services agency.

27 (4) "Director" means the state chief information officer, who is  
28 the director of the consolidated technology services agency.

29 (5) "Enterprise architecture" means an ongoing activity for  
30 translating business vision and strategy into effective enterprise  
31 change. It is a continuous activity. Enterprise architecture creates,  
32 communicates, and improves the key principles and models that  
33 describe the enterprise's future state and enable its evolution.

34 (6) "Equipment" means the machines, devices, and transmission  
35 facilities used in information processing, including but not limited  
36 to computers, terminals, telephones, wireless communications system  
37 facilities, cables, and any physical facility necessary for the  
38 operation of such equipment.

1 (7) "Information" includes, but is not limited to, data, text,  
2 voice, and video.

3 (8) "Information security" means the protection of communication  
4 and information resources from unauthorized access, use, disclosure,  
5 disruption, modification, or destruction in order to:

6 (a) Prevent improper information modification or destruction;

7 (b) Preserve authorized restrictions on information access and  
8 disclosure;

9 (c) Ensure timely and reliable access to and use of information;  
10 and

11 (d) Maintain the confidentiality, integrity, and availability of  
12 information.

13 (9) "Information technology" includes, but is not limited to, all  
14 electronic technology systems and services, automated information  
15 handling, system design and analysis, conversion of data, computer  
16 programming, information storage and retrieval, telecommunications,  
17 requisite system controls, simulation, electronic commerce, radio  
18 technologies, and all related interactions between people and  
19 machines.

20 (10) "Information technology portfolio" or "portfolio" means a  
21 strategic management process documenting relationships between agency  
22 missions and information technology and telecommunications  
23 investments.

24 (11) "K-20 network" means the network established in RCW  
25 43.41.391.

26 (12) "Local governments" includes all municipal and quasi-  
27 municipal corporations and political subdivisions, and all agencies  
28 of such corporations and subdivisions authorized to contract  
29 separately.

30 (13) "Office" means the office of the state chief information  
31 officer within the consolidated technology services agency.

32 (14) "Oversight" means a process of comprehensive risk analysis  
33 and management designed to ensure optimum use of information  
34 technology resources and telecommunications.

35 (15) "Proprietary software" means that software offered for sale  
36 or license.

37 (16) "Public agency" means any agency of this state or another  
38 state; any political subdivision or unit of local government of this  
39 state or another state including, but not limited to, municipal  
40 corporations, quasi-municipal corporations, special purpose

1 districts, and local service districts; any public benefit nonprofit  
2 corporation; any agency of the United States; and any Indian tribe  
3 recognized as such by the federal government.

4 (17) "Public benefit nonprofit corporation" means a public  
5 benefit nonprofit corporation as defined in RCW 24.03.005 that is  
6 receiving local, state, or federal funds either directly or through a  
7 public agency other than an Indian tribe or political subdivision of  
8 another state.

9 (18) "Public record" has the definitions in RCW 42.56.010 and  
10 chapter 40.14 RCW and includes legislative records and court records  
11 that are available for public inspection.

12 (19) "Public safety" refers to any entity or services that ensure  
13 the welfare and protection of the public.

14 (20) "Security incident" means an accidental or deliberative  
15 event that results in or constitutes an imminent threat of the  
16 unauthorized access, loss, disclosure, modification, disruption, or  
17 destruction of communication and information resources.

18 (21) "State agency" means every state office, department,  
19 division, bureau, board, commission, or other state agency, including  
20 offices headed by a statewide elected official.

21 (22) "Telecommunications" includes, but is not limited to,  
22 wireless or wired systems for transport of voice, video, and data  
23 communications, network systems, requisite facilities, equipment,  
24 system controls, simulation, electronic commerce, and all related  
25 interactions between people and machines.

26 (23) "Utility-based infrastructure services" includes personal  
27 computer and portable device support, servers and server  
28 administration, security administration, network administration,  
29 telephony, email, and other information technology services commonly  
30 used by state agencies.

31 (24) "Consent" means a clear, affirmative act establishing a  
32 freely given, specific, informed, and unambiguous indication of a  
33 consumer's agreement to the processing of personal data relating to  
34 the consumer, such as by a written statement or other clear,  
35 affirmative action.

36 (25) "Consumer" means a natural person who is a Washington  
37 resident. It does not include an employee or contractor of a business  
38 acting in their role as an employee or contractor.

39 (26) "Deidentified data" means data that: (a) Cannot be linked to  
40 a known natural person without additional information kept

1 separately; or (b)(i) has been modified to a degree that the risk of  
2 reidentification is small, or (ii) a state agency has committed to  
3 not attempt to reidentify.

4 (27) "Identified or identifiable natural person" means a person  
5 who can be identified, directly or indirectly, in particular by  
6 reference to an identifier such as a name, an identification number,  
7 specific geolocation data, or an online identifier.

8 (28) "Personal data" means any information collected by a state  
9 agency or entity relating to an identified or identifiable natural  
10 person. Personal data does not include deidentified data.

11 (29) "Personal information" means any information relating to an  
12 identified or identifiable natural person. Personal data does not  
13 include deidentified data or health care, financial, or educational  
14 data protected by federal law.

15 (30) "Process" or "processing" means any operation or set of  
16 operations that is performed on personal data or on sets of personal  
17 data, whether or not by automated means, such as collection,  
18 recording, organization, structuring, storage, adaptation or  
19 alteration, retrieval, consultation, use, disclosure by transmission,  
20 dissemination or otherwise making available, alignment or  
21 combination, restriction, deletion, or destruction.

22 (31) "Profiling" means any form of automated processing of  
23 personal data consisting of the use of personal data to evaluate  
24 certain personal aspects relating to a natural person, in particular  
25 to analyze or predict aspects concerning that natural person's  
26 economic situation, health, personal preferences, interests,  
27 reliability, behavior, location, or movements.

28 (32) "Restriction of processing" means the marking of stored  
29 personal data with the aim of limiting the processing of such  
30 personal data in the future.

31 (33) "Sale" means the exchange of personal data for monetary  
32 consideration to a third party for purposes of aggregating and  
33 licensing or disclosing personal data at the third party's discretion  
34 to additional third parties. "Sale" does not include the disclosure  
35 of personal data to a third party, such as another state agency or  
36 branch of government, with whom the consumer has a direct  
37 relationship for purposes of providing a product or service requested  
38 by the consumer or otherwise in a manner that is consistent with a  
39 consumer's reasonable expectations considering the context in which  
40 the consumer provided the personal data to the state agency.

1       (34) "Sensitive data" means personal data revealing racial or  
2 ethnic origin, religious or philosophical beliefs, and the processing  
3 of genetic data, biometric data for the purpose of uniquely  
4 identifying a natural person, data concerning a minor, data  
5 concerning health, or data concerning a natural person's sex life or  
6 sexual orientation.

7       NEW SECTION. Sec. 4. A new section is added to chapter 43.105  
8 RCW to read as follows:

9       (1) The sale of personal data to third parties by state agencies  
10 is prohibited except as authorized by law. For the avoidance of  
11 doubt, any such sale of personal data that fails to comply with the  
12 requirements of this chapter is impermissible.

13       (2) State agencies authorized by law to sell information  
14 containing the personal data of individuals to third parties must  
15 take affirmative steps, including but not limited to those set forth  
16 in this chapter, to protect such data from impermissible subsequent  
17 use, transfer, or sale by such third parties.

18       (3) Before completing a sale of personal data or confidential  
19 data to an entity other than the subject of such data, a state agency  
20 must confirm that the conditions under which the data is to be used  
21 are documented in a contract involving one or more state agencies.

22       (a) The contract must include the following requirements at a  
23 minimum:

24       (i) A data recipient must undergo both permissible use and data  
25 security audits prior to receiving data and on a reoccurring basis;

26       (ii) A data security audit must verify at a minimum compliance  
27 with the data security standards adopted by the office of the chief  
28 information officer, or equivalent;

29       (iii) A permissible use audit must verify at a minimum compliance  
30 with permissible use standards adopted by the state agency;

31       (iv) A data recipient that shares data with other entities must:

32       (A) Enter into a contract that includes at a minimum the data  
33 security, permissible use, and audit requirements set forth in the  
34 contract;

35       (B) Require the data recipient to ensure that subsequent  
36 recipients comply with the data security, permissible use, and audit  
37 requirements; and

38       (C) Other requirements as may be required by the office of the  
39 chief information officer; and

1 (v) A provision that the cost of the audits performed pursuant to  
2 this subsection must be borne by the data recipient. A new data  
3 recipient must bear the initial cost to set up a system to disburse  
4 the data to the data recipient.

5 (b) Audits required under this section must be conducted in  
6 accordance with professional audit standards by individuals with  
7 nationally recognized certifications relevant to the type of audit  
8 performed.

9 (c) A state agency may accept an audit meeting the requirements  
10 of this section that was conducted within the previous year.

11 (4)(a) State agencies may charge a fee in connection with the  
12 dissemination of personal data under this section for the purpose of  
13 recovering processing costs.

14 (b) State agencies must use any moneys collected under this  
15 subsection solely for the purposes of technology improvement, data  
16 management, and data audit functions.

17 (5) If a list or other compilation of personal data is used for  
18 any purpose other than that authorized in this section, the agent or  
19 contractor responsible for the unauthorized disclosure or use must be  
20 denied further access to such information by the state agency.

21 (6) Nothing in this section shall be construed to relieve any  
22 state agency of any obligation imposed by chapter 19.255 RCW.

23 (7) The requirements of this section do not apply to the  
24 following:

25 (a) Public records disclosed pursuant to the public records act,  
26 chapter 42.56 RCW, and related law;

27 (b) Release of records for research pursuant to chapter 42.48  
28 RCW;

29 (c) Review, release, or correction of data by the individual who  
30 is the subject of the data, pursuant to RCW 43.105.365;

31 (d) Voluntary publication of open data via state systems that are  
32 widely accessible by the public pursuant to RCW 43.105.365; or

33 (e) Campaign disclosure and contribution data published pursuant  
34 to chapter 42.17A RCW.

35 NEW SECTION. **Sec. 5.** A new section is added to chapter 43.105  
36 RCW to read as follows:

37 The office of privacy and data protection must publish among its  
38 privacy principles and best practices the following statement of

1 principles to promote responsible stewardship of the state's  
2 structured data assets:

3 (1) Data minimization: Data access, collection, and processing  
4 should be kept to the minimum amount necessary to fulfill its  
5 purpose.

6 (a) The retention of data should have a legitimate and fair  
7 basis, including beyond the purposes for which access to the data was  
8 originally granted, to ensure that no extra or just-in-case data set  
9 is stored.

10 (b) Any data retention should be also considered in light of the  
11 potential risks, harms, and benefits. The data should be permanently  
12 deleted upon conclusion of the time period needed to fulfill its  
13 purpose.

14 (2) Due diligence: Third-party collaborators engaging in data use  
15 should act in compliance with relevant laws, including privacy laws,  
16 as well as the highest standards of confidentiality.

17 (a) Third-party collaborators' actions should adhere to the same  
18 principles as public agencies.

19 (b) Legally binding agreements outlining parameters for data  
20 access and handling, including but not limited to data security, data  
21 formats, data transmission, fusion, analysis, validation, storage,  
22 retention, reuse, licensing, and disposition, should be established  
23 to ensure reliable and secure access to data provided by third-party  
24 collaborators.

25 (3) Sensitive data and sensitive contexts: Stricter standards of  
26 data protection should be employed while obtaining, accessing,  
27 collecting, analyzing, or otherwise using data on vulnerable  
28 populations and persons at risk, children and young people, or any  
29 other sensitive data.

30 (4) Data quality: Data and information are critical to effective  
31 business decision making in government and should be maintained in a  
32 manner appropriate to meet business needs.

33 (a) Data and information that is used by multiple applications or  
34 shared across business units should be defined and managed from an  
35 enterprise perspective and fit for a variety of purposes.

36 (b) All data-related activities should be designed, carried out,  
37 reported, and documented accurately. More specifically, data should  
38 be validated for accuracy, relevancy, sufficiency, integrity,  
39 completeness, usability, validity, and coherence, and be kept up to  
40 date.



1 (c) Data quality should be carefully considered in light of the  
2 risks that the use of low-quality data for decision making can create  
3 for individuals and groups.

4 (5) Open data, transparency and accountability: Transparency is a  
5 critical element of accountability. Being transparent about data use,  
6 including but not limited to publishing data sets or publishing an  
7 organization's data use practices, is generally encouraged, but  
8 should be balanced against privacy, justice, and environmental  
9 stewardship.

10 (a) Except in cases where there is a legitimate reason not to do  
11 so, the existence, description, meaning, authorship, location, age,  
12 and purpose of data use should be publicly disclosed and described in  
13 a clear and nontechnical language suitable for a general audience.

14 (b) Open data is an important driver of innovation, transparency,  
15 and accountability. Therefore, whenever possible, the data should be  
16 made open unless there are legitimate reasons not to do so.

17 (c) Disclosure of personal information through public data should  
18 be avoided or carefully assessed for potential risks and harms.

19 (6) Data security: Data security is crucial in ensuring data  
20 privacy and data protection. Taking into account available technology  
21 and cost of implementation, robust technical and organizational  
22 safeguards and procedures, including efficient monitoring of data  
23 access and data breach notification procedures, should be implemented  
24 to ensure proper data management throughout the data life cycle and  
25 prevent any unauthorized use, disclosure, or breach of personal data.

26 (a) No deidentified data should knowingly and purposely be  
27 reidentified, unless there is a legitimate, lawful, and fair basis  
28 for doing so.

29 (b) Data access should be limited to authorized personnel, based  
30 on the "need-to-know" principle.

31 (c) Personnel should undergo regular and systematic data privacy  
32 and data security trainings.

33 (d) Prior to data use, vulnerabilities of the security system,  
34 including but not limited to data storage and way of transfer, should  
35 be assessed.

36 NEW SECTION. **Sec. 6.** A new section is added to chapter 43.105  
37 RCW to read as follows:

38 State agencies shall facilitate requests to exercise the consumer  
39 rights set forth in subsections (1) through (6) of this section.

1 (1) On request from a consumer, a state agency must confirm  
2 whether or not personal data concerning the consumer is being  
3 processed by the state agency, including whether such personal data  
4 is sold to data brokers, and, where personal data concerning the  
5 consumer is being processed by the state agency, provide access to  
6 such personal data concerning the consumer.

7 (a) On request from a consumer, a state agency must provide a  
8 copy of the personal data undergoing processing. For any further  
9 copies requested by the consumer, the state agency may charge a  
10 reasonable fee based on administrative costs. Where the consumer  
11 makes the request by electronic means, and unless otherwise requested  
12 by the consumer, the information must be provided in a commonly used  
13 electronic form. A secure online portal satisfies the access  
14 provisions of this act. The portal may cover more than one state  
15 agency, provided there is secure access to accounts at separate  
16 agencies.

17 (b) This subsection does not adversely affect the rights of  
18 others and does not supersede any provision of the public records  
19 act, chapter 42.56 RCW.

20 (2) On request from a consumer, the state agency, without undue  
21 delay, must correct inaccurate personal data concerning the consumer.  
22 Providing secure access to an online account satisfies this  
23 requirement, as well as the subsequent requirements in this section.

24 (3) (a) On request from a consumer, a state agency must delete the  
25 consumer's personal data without undue delay where the personal data  
26 is no longer necessary in relation to the purposes for which the  
27 personal data was collected or otherwise processed.

28 (b) This subsection does not apply to the extent processing is  
29 necessary:

30 (i) For compliance with a legal obligation that requires  
31 processing by federal, state, or local law to which the state agency  
32 is subject or for the performance of a task carried out in the public  
33 interest or in the exercise of official authority vested in the state  
34 agency;

35 (ii) For reasons of public interest in the area of public health,  
36 where the processing is subject to suitable and specific measures to  
37 safeguard the rights of the consumer;

38 (iii) For archiving purposes in the public interest, scientific  
39 or historical research purposes, or statistical purposes, where the  
40 deletion of such personal data is likely to render impossible or

1 seriously impair the achievement of the objectives of the processing;  
2 or

3 (iv) For the establishment, exercise, or defense of legal claims.

4 (4) (a) On request from a consumer, the state agency must restrict  
5 processing if one of the following grounds applies:

6 (i) The accuracy of the personal data is contested by the  
7 consumer, for a period enabling the state agency to verify the  
8 accuracy of the personal data;

9 (ii) The processing is unlawful and the consumer opposes the  
10 deletion of the personal data and requests the restriction of  
11 processing instead; or

12 (iii) The state agency no longer needs the personal data for the  
13 purposes of the processing, but such personal data is required by the  
14 consumer for the establishment, exercise, or defense of legal claims.

15 (b) Where personal data is subject to a restriction of  
16 processing under this subsection, the personal data must, with the  
17 exception of storage, only be processed: (i) With the consumer's  
18 consent; (ii) for the establishment, exercise, or defense of legal  
19 claims; (iii) for the protection of the rights of another natural or  
20 legal person; or (iv) for reasons of important public interest under  
21 federal, state, or local law.

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

25 (5) Upon request by a consumer, the state agency must provide the  
26 consumer any personal data concerning such consumer that such  
27 consumer has provided to a state agency in a structured, commonly  
28 used, and machine-readable format if: (a) (i) The processing of such  
29 personal data is necessary for the performance of a contract to which  
30 the consumer is a party or (ii) in order to take steps at the request  
31 of the consumer prior to entering into a contract; and (b) the  
32 processing is carried out by automated means.

33 (6) A state agency must communicate any correction, deletion, or  
34 restriction of processing carried out in accordance with subsection  
35 (2), (3), or (4) of this section to each third-party recipient to  
36 whom the personal data has been disclosed, including third parties  
37 that received the data through a sale, unless this proves impossible  
38 or involves disproportionate effort. The state agency must inform the  
39 consumer about such third-party recipients, if any, if the consumer  
40 requests such information.

1 (7) A state agency must provide information on action taken on a  
2 request under subsections (1) through (6) of this section without  
3 undue delay and in any event within thirty days of receipt of the  
4 request. That period may be extended by sixty additional days where  
5 necessary, taking into account the complexity and number of the  
6 requests. The state agency must inform the consumer of any such  
7 extension within thirty days of receipt of the request with the  
8 reasons for the delay. Where the consumer makes the request by  
9 electronic means, the information must be provided by electronic  
10 means where possible, unless otherwise requested by the consumer.

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

16 (b) Information provided under this section must be provided by  
17 the state agency free of charge to the consumer. Where requests from  
18 a consumer are manifestly unfounded or excessive, in particular  
19 because of their repetitive character, the state agency may either:

20 (i) Charge a reasonable fee taking into account the  
21 administrative costs of providing the information or communication or  
22 taking the action requested; or

23 (ii) Refuse to act on the request. The state agency bears the  
24 burden of demonstrating the manifestly unfounded or excessive  
25 character of the request.

26 (c) Where the state agency has reasonable doubts concerning the  
27 identity of the consumer making a request under this subsection and  
28 subsections (1) through (6) of this section, the state agency may  
29 request the provision of additional information necessary to confirm  
30 the identity of the consumer.

31 NEW SECTION. **Sec. 7.** A new section is added to chapter 43.105  
32 RCW to read as follows:

33 (1) State agencies must be transparent and accountable for their  
34 processing of personal data by making available in a form that is  
35 reasonably accessible to consumers a clear, meaningful privacy notice  
36 that includes:

37 (a) The categories of personal data collected by the state  
38 agency;

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

3 (c) The rights that consumers may exercise pursuant to section 5  
4 of this act, if any;

5 (d) The categories of personal data that the state agency shares  
6 with third parties, if any; and

7 (e) The categories of third parties, if any, with whom the state  
8 agency shares personal data.

9 (2) State agencies that engage in profiling must disclose such  
10 profiling to the consumer at or before the time personal data is  
11 obtained, including meaningful information about the logic involved  
12 and the significance and envisioned consequences of the profiling.

13 NEW SECTION. **Sec. 8.** A new section is added to chapter 43.105  
14 RCW to read as follows:

15 (1) State agencies must certify compliance with the requirements  
16 of this chapter.

17 (2) By June 30, 2024, the office of privacy and data protection  
18 must provide a design template for consumer access to data and  
19 develop compliance criteria to meet the requirements of this chapter.

20 (3) This chapter applies to all state agencies. Agencies may  
21 request a waiver for hardship or inability to comply for special  
22 circumstances. The office of privacy and data protection must  
23 determine the waiver and must not unreasonably withhold it. The  
24 waiver may take the form of an extension of time to comply with  
25 specific provisions.

26 NEW SECTION. **Sec. 9.** Section 6 of this act takes effect January  
27 1, 2025.

--- END ---