Definitions *Sec. 3*	2SSB 5376	Amendment H-2436.1
"*Business purposes*"	Auditing related to a current interaction with the consumer and concurrent transactions including, but not limited to, counting ad impressions, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards. Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.	Auditing related to a current interaction with the consumer and concurrent transactions including, but not limited to, counting ad impressions, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards. Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity, and notifying consumers of illegal activity that impacts personal data.
"*Consent*"	A clear affirmative act signifying a specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action.	A clear affirmative act signifying a freely given, specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action.
"*Data Broker*"	A business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. Providing publicly available information through real-time or near real-time alert services for health or safety purposes, and the collection and sale or licensing of brokered personal information incidental to conducting those activities, does not qualify the business as a data broker. The phrase "sells or licenses" does not include: (i) A one-time or occasional sale of assets that is not part of the ordinary conduct of the business; (ii) A sale or license of data that is merely incidental to the business; or (iii) Providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier.	A business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. Providing publicly available information through real-time or near real-time alert services for health or safety purposes, and the collection and sale or licensing of brokered personal information incidental to conducting those activities, does not qualify the business as a data broker. Providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier, does not qualify the business as a data broker.

"*Identified or identifiable natural person*"	A person who can be readily identified, directly or indirectly.	A person who can be readily identified, directly or indirectly, in particular by reference to an identifier, including, but not limited to a name, an online identifier, an identification number, or specific geolocation data.
"*Legal effects*"	n/a	"**Legal effects**" means, without limitation, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, and other similarly significant effects.
"*Personal data*"	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. For these purposes, "publicly available information" means information that is lawfully made available from federal, state, or local government records.	Any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include deidentified data.
"*Sale*"	The exchange of personal data for monetary consideration by the controller to a third party for purposes of licensing or selling personal data at the third party's discretion to additional third parties. **"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 or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personal data to the controller; (iii) the disclosure or transfer of personal data to an affiliate of the controller; or (iv) 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.	The exchange of personal data for consideration by the controller to a third party for purposes of licensing or selling personal data at the third party's discretion to additional third parties. **"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 or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personal data to the controller; (iii) the disclosure or transfer of personal data to an affiliate of the controller; or (iv) 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, if consumers are notified of the transfer of their data and of their rights under this chapter.

Jurisdictional Scope and Responsibility According to Role	2SSB 5376	Amendment H-2436.1
To whom obligations apply *Sec. 4*	**This chapter applies to legal entities** that conduct business in Washington or produce products or services that are intentionally targeted to residents of Washington, and that satisfy one or more of the following thresholds: (a) Controls or processes personal data of one hundred thousand consumers or more; or (b) Derives over fifty percent of gross revenue from the sale of personal data and processes or controls personal data of twenty-five thousand consumers or more.	**This chapter applies to legal entities** that conduct business in Washington or produce products or services that are intentionally targeted to residents of Washington.
Exempt entities and data	State and local governments Municipal corporations *See Sec. 4(2)(c) through Sec. 4(2)(h)* Certain information and entities that are subject to specified federal and state laws or regulations are exempt from the provisions of the bill.	State and local governments Municipal corporations *Sec. 4(2)* Certain information subject to specified federal and state laws or regulations are exempt from the provisions of the bill only if the information is collected, used, disclosed, maintained, or processed in compliance with and solely for the purposes of the specified statutory provisions applicable to that information.
Responsibility According to Role *Sec. 5*	**Controllers** are responsible for meeting the obligations established under this chapter. **Processors** are responsible under this act for adhering to the instructions of the controller and assisting the controller to meet its obligations under this chapter. Processing by a processor is governed by a contract between the controller and the processor that is binding on the processor and that sets out the processing instructions to which the processor is bound.	**Controllers** are responsible for meeting the obligations established under this chapter. **Processors** are responsible under this act for adhering to the instructions of the controller and assisting the controller to meet its obligations under this chapter. Processing by a processor is governed by a contract between the controller and the processor that is binding on the processor and that sets out the processing instructions to which the processor is bound. Third parties are responsible for assisting controllers and processors in meeting their obligations under this chapter with regard to personal data third parties receive from controllers or processors.

Consumer Rights *Sec. 6*	2SSB 5376	Amendment H-2436.1
Consumer Rights Generally	Controllers shall facilitate verified requests to exercise the consumer rights.	A consumer retains ownership interest in the consumer's personal data processed by a controller or a processor and may exercise any of the consumer rights by submitting to a controller a verified request that specifies which rights the consumer wishes to exercise.
The right to be informed about processing of personal data	*Sec. 6 (1)* Upon receiving a verified consumer request, **a controller must confirm** whether or not the consumer's personal data is being processed by the controller, including whether such personal data is sold to data brokers, and, where the consumer's personal data is being processed by the controller, **provide access** to such personal data that the controller maintains in identifiable form.	
The right to be informed about other recipients of personal data	*Sec. 6(7)* The controller must inform the consumer about third-party recipients or categories with whom the controller shares personal information, if any, if the consumer requests such information.	*Sec. 6(9)* Upon receiving a verified consumer request, a controller must inform the consumer about third-party recipients or categories of third-party recipients of the consumer's personal data, including third parties that received the data through a sale.
The right to correction	*Sec. 6(2)* Upon a verified request from a consumer, the controller, without undue delay, **must correct** inaccurate personal data that the controller maintains in identifiable form concerning the consumer. Taking into account the business purposes of the processing, the controller must complete incomplete personal data, including by means of providing a supplementary statement where appropriate.	*Sec. 6(3)* Upon receiving a verified consumer request, a controller **must correct** the consumer's inaccurate personal data that the controller maintains in identifiable form, or complete the consumer's incomplete personal data, including by means of providing a supplementary statement where appropriate.
The right of access	*Sec. 6(1)(a) & Sec. 6(2)* Upon receiving a verified consumer request, a controller **must provide**, in a commonly used electronic format, a copy of the consumer's personal data that is undergoing processing and that the controller maintains in identifiable form.	

The right to data portability	*Sec. 6(5)(a). See also Sec. 8(3) - Risk Assessments*. Upon a verified request from a consumer, the **controller must provide to the consumer**, if technically feasible and commercially reasonable, any personal data that the controller maintains in identifiable form concerning the consumer that such consumer has provided to the controller in a structured, commonly used, and machine-readable format **if** (i) (A) the processing of such personal data requires consent under [*Risk Assessments*] section of this act (B) the processing of such personal data is necessary for the performance of a contract to which the consumer is a party, or (C) in order to take steps at the request of the consumer prior to entering into a contract; and (ii) the processing is carried out by automated means.	*See Sec. 6(2) - The right of access* Upon receiving a verified consumer request, a controller **must provide**, in a commonly used electronic format, a copy of the consumer's personal data that is undergoing processing and that the controller maintains in identifiable form.
Limitations on the right to data portability	*Sec. 6(5)(b) & Sec. 6(5)(c)* Requests for personal data under this subsection must be without prejudice to the other rights granted in this chapter. The rights provided in this subsection do not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and must not adversely affect the rights of others.	No limitations specific to the right of access/data portability. *Sec. 6 (15)* Requests for personal data under this section must be without prejudice to the other rights granted in this chapter. *Sec. 6(19)* The rights provided in this section must not adversely affect the rights of others. *See also Sec. 11 - EXEMPTIONS.*

The right to deletion	*Sec. 6(3)(a). See also Sec. 8(3) - Risk Assessments*. Upon a verified request from a consumer, a controller must delete, without undue delay, the consumer's personal data that the controller maintains in identifiable form if one of the following grounds applies: (a) The personal data is no longer necessary for a business purpose, including the provision of a product or service to the consumer; (b) For processing that requires consent under [*Risk Assessments*] section of this act, the consumer withdraws consent to processing and there are no business purposes for the processing; (c) The consumer objects to the processing and (i) there are no business purposes for processing the personal data for the controller, the consumer whose personal data is being processed, or the public, for which the processing is necessary; or (ii) the processing is for targeted advertising; (d) The personal data has been unlawfully processed; or (e) The personal data must be deleted to comply with a legal obligation under federal, state, or local law to which the controller is subject.	*Sec. 6(4). See also Sec. 9(3) - Risk Assessments*. Upon receiving a verified consumer request, a controller must delete the consumer's personal data that the controller maintains in identifiable form, if one of the following grounds applies: (a) The personal data is no longer necessary in relation to the purposes for which it was collected or processed; (b) The consumer withdraws consent for processing that requires consent under [*Risk Assessments*] section of this act, and there are no other legitimate grounds for processing; (c) The consumer objects to processing and the processing is for direct marketing or targeted advertising purposes; (d) The personal data has been unlawfully processed; or (e) The personal data must be deleted to comply with a legal obligation under local, state, or federal law to which the controller is subject.

Limitations on the right to deletion	*Sec. 6(3)(c)* [*The right to deletion*] does not apply to the extent processing is necessary: (i) For exercising the right of free speech; (ii) For compliance with a legal obligation that requires processing of personal data by federal, state, or local law, or regulation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (iii) For reasons of public interest in the area of public health, where the processing (A) is subject to suitable and specific measures to safeguard the rights of the consumer; and (B) is under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law; (iv) For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where the deletion of such personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing; (v) For the establishment, exercise, or defense of legal claims; (vi) To detect or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or identify, investigate, or prosecute those responsible for that activity; or (vii) For a data broker that received the personal data from third parties and is acting as a controller, solely to prevent the personal data from reappearing in the future, in which case the controller shall instead comply with the requirements in subsection (4) of this section [*restriction of processing*].	*See Sec. 11 - EXEMPTIONS* No limitations specific to the right to deletion. .

The right to deletion -- notifying other controllers, processors, and third parties	*Sec. 6(3)(b)* Where the controller is obliged to delete personal data that the controller maintains in identifiable form under this section that has been disclosed to third parties by the controller, including data brokers that received the personal data through a sale, the controller must take reasonable steps, which may include technical measures, to inform other controllers of which it is aware that are processing such personal data, and that received such personal data from the controller or are processing such personal data on behalf of the controller, that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data. Compliance with this obligation must take into account available technology and cost of implementation.	*Sec. 6(5)* Upon receiving a verified consumer request, a controller must take reasonable steps to inform other controllers or processors of which the controller is aware, and which are processing the consumer's personal data they received from the controller, that the consumer has requested deletion of any copies of or links to the consumer's personal data.
The right to object to processing	*Sec. 6(6)* A consumer may object through a verified request, on grounds relating to the consumer's particular situation, at any time to processing of personal data concerning such consumer. When a consumer objects to the processing of their personal data for targeted advertising, which includes the sale of personal data concerning the consumer to third parties for purposes of targeted advertising, the controller must no longer process the personal data subject to the objection for such purpose and must take reasonable steps to communicate the consumer's objection, unless it proves impossible or involves disproportionate effort, regarding any further processing of the consumer's personal data for such purposes to any third parties to whom the controller sold the consumer's personal data for such purposes. If a consumer objects to processing for any purposes, other than targeted advertising, the controller may continue processing the personal data subject to the objection if the controller can demonstrate a legitimate ground to process such personal data that overrides the potential risks to the rights of the consumer associated with the processing, or if another exemption in this chapter applies.	*Sec. 6(8)* Upon receiving a verified consumer request, a controller must stop processing personal data of the consumer who objects to such processing, including the selling of the consumer's personal data to third parties for purposes of direct marketing or targeted advertising, without regard to the source of data.

The right to object to processing -- notifying third parties	*Sec. 6(6)* When a consumer objects to the processing of their personal data for targeted advertising, which includes the sale of personal data concerning the consumer to third parties for purposes of targeted advertising, the controller must no longer process the personal data subject to the objection for such purpose and must take reasonable steps to communicate the consumer's objection, unless it proves impossible or involves disproportionate effort, regarding any further processing of the consumer's personal data for such purposes to any third parties to whom the controller sold the consumer's personal data for such purposes. Third parties must honor objection requests pursuant to this subsection received from third-party controllers.	*Sec. 6(10)* A controller must take reasonable steps to communicate a consumer's objection to processing to third parties to whom the controller sold the consumer's personal data and who must honor objection requests received from the controller.
The right to restrict processing -- when processing must be restricted	*Sec. 6(4)(a)* Upon a verified request from a consumer, the controller **must restrict processing** of personal data that the controller maintains in identifiable form if the purpose for which the personal data is: (i) not consistent with a purpose for which the personal data was collected; (ii) not consistent with a purpose disclosed to the consumer at the time of collection or authorization; or (iii) unlawful.	*Sec. 6(6)(a)* Upon receiving a verified consumer request, a controller **must restrict processing** of the consumer's personal data if the purpose for which the personal data is being processed is: (i) Inconsistent with a purpose for which the personal data was collected; (ii) inconsistent with a purpose disclosed to the consumer at the time of collection or authorization; (iii) inconsistent with exercising the right of free speech; or (iv) unlawful.

The right to restrict processing -- when processing may continue	*Sec. 6(4)(b) and (c)* Where personal data is subject to a restriction of processing under this subsection, the personal data must, with the exception of storage, only be processed: (i) with the consumer's consent; (ii) for the establishment, exercise, or defense of legal claims; (iii) for the protection of the rights of another natural or legal person; (iv) for reasons of important public interest under federal, state, or local law; (v) to provide products or services requested by the consumer; or (vi) for another purpose set forth in subsection (3)(c) of this section. [*See the limitations on the right to deletion above*] A consumer who has obtained restriction of processing pursuant to this subsection must be informed by the controller before the restriction of processing is lifted.	*Sec. 6(6)(b) & Sec. 6(7)* Where personal data is subject to a restriction of processing under this subsection, the personal data must, with the exception of storage, only be processed: (i) with consumer's consent; (ii) for the establishment, exercise or defense of legal claims; (iii) for the protection of the rights of another natural or legal person; (iv) for reasons of important public interest under federal, state, or local law; (v) to provide products or services requested by the consumer; or (vi) for another purpose set forth in section 11 of this act. [*See Sec. 11 - EXEMPTIONS*] A controller must inform the consumer before any restriction of processing is lifted.
Communicating a consumer request to others	*Sec. 6(7)* A controller **must communicate** any correction, deletion, or restriction of processing carried out in accordance with subsections (2), (3), or (4) of this section **to each third-party recipient** to whom the controller knows the personal data has been disclosed, including third parties that received the data through a sale, **within one year preceding the verified request** unless this proves functionally impractical, technically infeasible, or involves disproportionate effort, or the controller knows or is informed by the third party that the third party is not continuing to use the personal data.	*Sec. 6(12)* A controller **must communicate** any correction, deletion, or restriction of processing carried out pursuant to a verified consumer request **to each third party** to whom the controller knows the consumer's personal data has been disclosed **within one year preceding the verified request**, including third parties that received the data through a sale.

General limitations on consumer rights	*See above for limitations on the right to deletion and the right to data portability.*	*Sec. 6 (15)* Requests for personal data under this section must be without prejudice to the other rights granted in this chapter. *Sec. 6(19)* The rights provided in this section must not adversely affect the rights of others.
Notifying consumers of their rights	No comparable provisions	*Sec. 6(17)* All policies adopted and used by a controller to comply with this section [*Consumer Rights*] must be publicly available on the controller's web site and included in the controller's online privacy policy.
Acting on a consumer's request	*Sec. 6(8) & Sec. 6(8)(a)* A controller must provide information on action taken on a verified request without undue delay and in any event **within 30 days** of receipt of the request. That period **may be extended by 60 additional days** where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any such extension within 30 days of receipt of the request, together with the reasons for the delay. If a controller does not take action on the request of a consumer, the controller must inform the consumer without undue delay and at the latest within 30 days of receipt of the request of the reasons for not taking action and any possibility for internal review of the decision by the controller. Where the consumer makes the request by electronic means, the information must be provided by electronic means where possible, unless otherwise requested by the consumer.	*Sec. 6(11)* A controller must take action on a consumer's request without undue delay and **within 30 days** of receiving the request. The request fulfillment period **may be extended by 60 additional days** where reasonably necessary, taking into account the complexity of the request. Within 30 days of receiving a consumer request, a controller must inform the consumer about: (i) Any fulfillment period extension, together with the reasons for the delay; or (ii) The reasons for not taking action on the consumer's request and any possibility for internal review of the decision by the controller.

Verifying the identity of a consumer	*Sec. 6(8)(c) & Sec. 6(14)* Where a controller has reasonable doubts concerning the identity of the consumer making a request under this section, the controller may request the provision of additional information necessary to confirm the identity of the consumer.	
Charging a fee to fulfill a consumer request	*Sec. 6(8)(b)* Information provided under this section must be provided by the controller **free of charge** to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (i) Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (ii) refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.	*Sec. 6(13)* Information provided under this section must be provided by the controller **free of charge** to the consumer. Where requests from a consumer are manifestly unfounded or excessive, the controller may refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

Transparency and Compliance	2SSB 5376	Amendment H-2436.1
Privacy Notice	*Sec. 7(1)* Controllers must be transparent and accountable for their processing of personal data, by making available in a form that is reasonably accessible to consumers a clear, meaningful privacy notice that includes: (a) The categories of personal data collected by the controller; (b) The purposes for which the categories of personal data is used and disclosed to third parties, if any; (c) The rights that consumers may exercise pursuant to section 6 of this act, if any; (d) The categories of personal data that the controller shares with third parties, if any; and (e) The categories of third parties, if any, with whom the controller shares personal data.	*Sec. 7(1)* Controllers must be transparent and accountable for their processing of personal data, by making available in a form that is reasonably accessible to consumers a clear, meaningful privacy notice that includes: (a) The categories of personal data collected by the controller; (b) The purposes for which the categories of personal data is used and disclosed to third parties, if any; (c) The rights that consumers may exercise pursuant to section 6 of this act, if any; (d) The categories of personal data that the controller shares with third parties, if any; (e) The categories of third parties, if any, with whom the controller shares personal data; and (f) The process by which a consumer may request to exercise the rights under section 6 of this act, including a process by which a consumer may appeal a controller's action with regard to the consumer's request.
Transparency about selling data	*Sec. 7(2)* If a controller sells personal data to data brokers or processes personal data for targeted advertising, it must disclose such processing, as well as the manner in which a consumer may exercise the right to object to such processing, in a clear and conspicuous manner.	*Sec. 7(2)* If a controller sells personal data to data brokers or processes personal data for direct marketing purposes, including targeted advertising, it must disclose such processing, as well as the manner in which a consumer may exercise the right to object to such processing, in a clear and conspicuous manner.
Compliance	No comparable provisions	*Sec. 8* (1) Controllers must develop and make publicly available an annual plan for complying with the obligations under this chapter. (2) A controller that has developed a compliance plan for the European general data protection regulation 2016/679 may use that plan for purposes of subsection (1) of this section. (3) Controllers may report metrics on their public web site to exemplify and support their compliance plans.

Risk Assessments and Deidentified Data	2SSB 5376	Amendment H-2436.1
Risk Assessments	*Sec. 8* (1) Controllers must conduct, to the extent not previously conducted, a risk assessment of each of their processing activities involving personal data and an additional risk assessment any time there is a change in processing that materially increases the risk to consumers. Such risk assessments must take into account the type of personal data to be processed by the controller, including the extent to which the personal data is sensitive data or otherwise sensitive in nature, and the context in which the personal data is to be processed. (2) Risk 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 factor into this assessment by the controller. (3) If the risk assessment conducted under subsection (1) of this section determines that the potential risks of privacy harm to consumers are substantial and outweigh the interests of the controller, consumer, other stakeholders, and the public in processing the personal data of the consumer, the controller may only engage in such processing with the consent of the consumer or if another exemption under this chapter applies. To the extent the controller seeks consumer consent for processing, such consent shall be as easy to withdraw as to give.	*Sec. 9* (1) Controllers must produce a risk assessment of each of their processing activities involving personal data and an additional risk assessment any time there is a change in processing that materially increases the risk to consumers. The risk assessments must take into account the: (a) Type of personal data to be processed by the controller; (b) Extent to which the personal data is sensitive data or otherwise sensitive in nature; and (c) Context in which the personal data is to be processed. (2) Risk assessments conducted under subsection (1) of this section must: (a) 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 the processing, as mitigated by safeguards that can be employed by the controller to reduce risks; and (b) Factor in 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. (3) If the risk assessment conducted under subsection (1) of this section determines that the potential risks of privacy harm to consumers are substantial and outweigh the interests of the controller, consumer, other stakeholders, and the public in processing the personal data of the consumer, the controller may only engage in such processing with the consent of the consumer. To the extent the controller seeks consumer consent for processing, consent must be as easy to withdraw as to give.

	(4) Processing for a business purpose shall be presumed to be permissible unless: (a) It involves the processing of sensitive data; and (b) the risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards.	(4) Processing data for a business purpose must be described in the risk assessment, but is presumed permissible unless: (a) It involves the processing of sensitive data; (b) the risk of processing cannot be reduced through the use of appropriate administrative and technical safeguards; (c) consent was not given; or (d) processing is inconsistent with consent given.
Deidentified Data	*Sec. 9* A controller or processor that uses deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified data is subject, and must take appropriate steps to address any breaches of contractual commitments.	*Sec. 10* A controller or processor that uses, sells, or shares deidentified data shall: (1) Provide by contract that third parties must not re-identify deidentified data received from a controller or a processor; (2) Exercise reasonable oversight to monitor compliance with any contractual commitments to which deidentified data is subject; and (3) Take appropriate steps to address any breaches of contractual commitments to which deidentified data is subject.

Exemptions	2SSB 5376	Amendment H-2436.1
Exemptions -- Generally	*Sec. 10(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; (b) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities; (c) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local law; (d) Investigate, exercise, or defend legal claims; (e) Prevent or detect identity theft, fraud, or other criminal activity or verify identities; (f) Perform a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract; (g) Protect the vital interests of the consumer or of another natural person; (h) Perform a task carried out in the public interest or in the exercise of official authority vested in the controller; (i) Process personal data of a consumer for one or more specific purposes where the consumer has given their consent to the processing; or (j) Prevent, detect, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action. *See also Sec. 6 - Consumer Rights - Limitations on the right to deletion and the right to data portability.*	*Sec. 11(1)* The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to: (a) Engage in processing that is necessary for reasons of public health interest, where the processing: (i) Is subject to suitable and specific measures to safeguard consumer rights; and (ii) is under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law; (b) Engage in processing that is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where the deletion of personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing; (c) Comply with federal, state, or local laws, rules, or regulations; (d) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities; (e) Establish, exercise, or defend legal claims; (f) Safeguard intellectual property rights; (g) Temporarily prevent, detect, or respond to security incidents; (h) Protect against malicious, deceptive, fraudulent, or illegal activity, or identify, investigate, or prosecute those responsible for that illegal activity; (i) Perform a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract; (j) Protect the vital interests of the consumer or of another natural person; (k) Process personal data of a consumer for one or more specific purposes where the consumer has given and has not withdrawn their consent to the processing; or (l) Assist another controller, processor, or third party with any of the activities under this subsection.

Exemptions - Evidentiary privilege	*Sec. 10(2) & Sec. 11(2)* The obligations imposed on controllers or processors under this chapter do not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under Washington law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Washington law as part of a privileged communication.
Exemptions - Disclosing personal data to third parties	*Sec. 10(3) & Sec. 11(3)* A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this chapter is not in violation of this chapter, including under [*Liability*] section of this act, if the recipient processes such personal data in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor is likewise not liable under this chapter, including under [*Liability*] section of this act, for the obligations of a controller or processor to which it provides services.
Exemptions - Other	*Sec. 10(4)-(5) & Sec. 11(4)-(5)* This chapter does not require a controller or processor to do the following: (a) Reidentify deidentified data; (b) Retain, link, or combine personal data concerning a consumer that it would not otherwise retain, link, or combine in the ordinary course of business; (c) Comply with a request to exercise any of the rights under section 6 of this act if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request. Obligations imposed on controllers and processors under this chapter do not: (a) Adversely affect the rights or freedoms of any persons; or (b) Apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

Facial Recognition Technology	2SSB 5376	Amendment H-2436.1
Facial Recognition	*Sec. 14*	*Sec. 12*
		Prior to using facial recognition technology, controllers and processors must verify, through independent third-party testing or auditing, that no statistically significant variation occurs in the accuracy of the facial recognition technology on the basis of race, skin tone, ethnicity, gender, or age of the individuals portrayed in testing images.
	Controllers using facial recognition for profiling must employ meaningful human review prior to making final decisions based on such profiling where such final decisions produce legal effects concerning consumers or similarly significant effects concerning consumers. Decisions producing legal effects or similarly significant effects shall include, but not be limited to, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.	Controllers may not use facial recognition for profiling and must employ meaningful human review prior to making final decisions based on the use of facial recognition technology where final decisions produce legal effects or similarly significant effects concerning consumers, including, but not limited to, denial of consequential service or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.
	Processors that provide facial recognition services must provide documentation that includes general information that explains the capabilities and limitations of the technology in terms that customers and consumers can understand.	Processors that provide facial recognition services must provide documentation that includes general information that explains the capabilities and limitations of the technology in terms that reasonable customers and consumers can understand.
	Processors that provide facial recognition services must prohibit, in the contract required by section 5 of this act, the use of such facial recognition services by controllers to unlawfully discriminate under federal or state law against individual consumers or groups of consumers.	Processors that provide facial recognition services must prohibit, in the contract required by section 5 of this act, the use of such facial recognition services by controllers to unlawfully discriminate under federal or state law against individual consumers or groups of consumers.
	Controllers must obtain consent from consumers prior to deploying facial recognition services in physical premises open to the public. The placement of conspicuous notice in physical premises that clearly conveys that facial recognition services are being used constitute a consumer's consent to the use of such facial recognition services when that consumer enters those premises that have such notice.	Controllers must obtain consent from consumers prior to deploying facial recognition services in physical premises open to the public. The placement of conspicuous notice in physical premises that clearly conveys that facial recognition services are being used does not constitute a consumer's clear and affirmative consent to the use of facial recognition services when that consumer enters a premises that have such a notice.

	Providers of commercial facial recognition services that make their technology available as an online service for developers and customers to use in their own scenarios must make available an application programming interface or other technical capability, chosen by the provider, to enable third parties that are legitimately engaged in independent testing to conduct reasonable tests of those facial recognition services for accuracy and unfair bias.	Active, informed consumer consent is required before facial recognition may be used or any data resulting from the use of facial recognition may be processed. Providers of commercial facial recognition services that make their technology available as an online service for developers and customers to use in their own scenarios must make available an application programming interface or other technical capability, chosen by the provider, to enable third parties that are legitimately engaged in independent testing to conduct reasonable tests of those facial recognition services for accuracy and unfair bias. Providers must track and make reasonable efforts to correct instances of bias identified by this independent testing. Controllers, processors, and providers of facial recognition services must notify consumers if an automated decision system makes decisions affecting the constitutional or legal rights, duties, or privileges of any Washington resident. Unless required by a court order, nothing in this section requires providers of facial recognition services to reveal proprietary data, trade secrets, intellectual property, or information that increases the risk of cyberattacks, including cyberattacks related to unique methods of conducting business, data unique to the product or services, or determination of prices or rates to be charged for products or services.
Facial Recognition - Use by state and local government agencies	*Sec. 15* State and local government agencies shall not use facial recognition technology to engage in ongoing surveillance of specified individuals in public spaces, unless such use is in support of law enforcement activities and either: (a) A court order has been obtained to permit the use of facial recognition services for that ongoing surveillance; or (b) Where there is an emergency involving imminent danger or risk of death or serious physical injury to a person.	*Sec. 16* State and local government agencies may not use facial recognition technology to engage in ongoing surveillance of specified individuals in public places, unless such a use is in support of law enforcement activities and either: (a) A court issued a warrant based on probable cause to permit the use of facial recognition technology for that surveillance during a specified time frame; or (b) There is an emergency involving imminent danger or risk of death or serious injury to a person.

Liability and Enforcement	2SSB 5376	Amendment H-2436.1
Liability	*Sec. 11* This chapter does not serve as the basis for a private right of action under this chapter or any other law. Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this chapter, the liability shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.	*Sec. 13* *See Sec. 14(3)-(5) for provisions related to private right of action* Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this chapter, the liability shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.
Enforcement - Violations	*Sec. 12(3)* A controller or processor is in violation of this chapter if it fails to cure any alleged violation of this act within thirty days after receiving notice of alleged noncompliance.	*Sec. 14(6)* A controller or processor is in violation of this chapter if it fails to cure any alleged violation of this act within thirty days after receiving notice of alleged noncompliance. Curing a violation entails instituting mitigations to stop an ongoing violation such that there is minimal likelihood of negative impact on consumers that were affected by the violation.
Enforcement by the Attorney General	*Sec. 12(1)-(2) & Sec. 14(1)-(2)* The legislature finds that 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. A violation of this chapter is not reasonable in relation to the development and preservation of business and 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. The Attorney General may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this chapter.	

Enforcement through private action	*Sec. 11(1)* This chapter does not serve as the basis for a private right of action under this chapter or any other law.	*Sec. 14(3)-(5)* Prior to bringing an action for violations of this chapter, a consumer must provide a controller with a written notice identifying the specific provisions of this chapter that the consumer alleges have been or are being violated. In the event a cure is possible and the controller does not cure the noticed violation within thirty days, the consumer must notify the attorney general of the consumer's intent to bring an action. Upon receiving such notice, the attorney general must either: (a) Notify the consumer within thirty days that the attorney general intends to bring an action under [*Enforcement by the Attorney General*] subsections of this section and that the consumer may not proceed with a separate action; or (b) Refrain from acting within thirty days and allow the consumer to bring an action. In an action brought under this chapter, each party is responsible for its own attorney's fees and legal costs.
Enforcement - Penalties	*Sec. 12(3) & Sec. 14(7)* Any controller or processor that violates this chapter is subject to an injunction and liable for a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation. *Sec. 12(4) & Sec.14(8)* The consumer privacy account is created in the state treasury. All receipts from the imposition of civil penalties pursuant to an action by the attorney general under this chapter must be deposited into the account. Moneys in the account may be spent only after appropriation. Expenditures from the account may be used to fund the office of privacy and data protection as established under RCW 43.105.369.	

	2SSB 5376	Amendment H-2436.1
Office of Privacy and Data Protection	*Sec. 16(8)-(9)* The office of privacy and data protection must conduct an analysis on the public sector use of facial recognition. By September 30, 2023, the office of privacy and data protection must submit a report of its findings to the appropriate committees of the legislature. The office of privacy and data protection, in consultation with the attorney general, must by rule (a) establish any exceptions to this chapter necessary to comply with state or federal law by the effective date of this section and as necessary thereafter, (b) clarify definitions of this chapter as necessary, and (c) create exemption eligibility requirements for small businesses and research institutions.	*Sec. 15(8)-(9)* The office of privacy and data protection must conduct an analysis on the public sector use of facial recognition. By September 30, 2022, the office of privacy and data protection must submit a report of its findings to the appropriate committees of the legislature. The office of privacy and data protection, in consultation with the attorney general, must by rule (a) clarify definitions of this chapter as necessary, and (b) create exemption eligibility requirements for small businesses and research institutions.
Preemption	*Sec. 13 & Sec. 17* 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.	
Other provisions	n/a	This act is subject to appropriations in the omnibus appropriations act. 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. If any provision of this act is found to be in conflict with federal or state law or regulations, the conflicting provision of this act is declared to be inoperative.
Effective date	July 31, 2021	July 30, 2020