PRIVACY COMPARISON: 2SSB 6281 and SHB 2742

Definitions *Section 3*	**2SSB 6281**	**SHB 2742**	**Relevant bill provisions**
"Child"	"Child" means any natural person under thirteen years of age.	"Child" means any natural person under eighteen years of age.	*Sec. 3(34)* Personal data from a known child is included in the definition of "sensitive data" *Sec. 6* In the case of processing personal data of a known child, the parent or legal guardian of the known child shall exercise the consumer personal data rights on the child's behalf. *Sec. 8(7)* Controllers may not process sensitive data without consumer consent or parental consent (in accordance with COPPA), in the case of processing personal data of a child.
"Consumer"	"Consumer" means a natural person who is a Washington resident acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.	"Consumer" means a natural person who is a Washington resident acting only in an individual or household context. It does not include a natural person acting in an employment context.	Used throughout the bill
"Deidentified data"	"Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to such person, provided that the controller that possesses the data: (a) Takes reasonable measures to ensure that the data cannot be associated with a natural person; (b) publicly commits to maintain and use the data only in a deidentified fashion and not attempt to reidentify the data; and	"Deidentified data" means data that cannot be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to such person, provided that the controller that possesses the data: (a) Takes measures to ensure that the data cannot be associated with a natural person, device, or household; (b) publicly commits to maintain and use the data only in a deidentified fashion and not attempt to reidentify the data; and	"Personal data" does not include deidentified data. *Sec. 7(1)* Controllers or processors are not required to reidentify deidentified data solely to comply with this act. *Sec. 7(3)* Controllers using deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which deidentified data

"Deidentified data" (cont'd)	(c) contractually obligates any recipients of the information to comply with all provisions of this subsection.	(c) contractually obligates any recipients of the information to comply with all provisions of this subsection.	are subject and must take appropriate steps to address any breaches of contractual commitments. *Sec. 9(2)* The use of deidentified data must be factored into a data protection assessment by a controller when identifying and weighing the benefits from the processing to the controller, consumer, other stakeholders, and the public against the potential risks to consumer rights.
"Personal data"	"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include deidentified data or publicly available information. "Publicly available information" means information that is lawfully made available from federal, state, or local government records.	"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include deidentified data or publicly available information. "Publicly available information" means information that is lawfully made available from federal, state, or local government records and not combined with personal data obtained from sources other than federal, state, or local government records.	Used throughout the bill
"Pseudonymous data"	"Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	"Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is not readily available and is subject to appropriate technical and organizational measures to ensure that the personal data cannot reasonably be attributed to an identified or identifiable natural person.	*Sec. 7(2)* Except for the right to opt out, consumer personal data rights do not apply to pseudonymous data where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

"Sale"	"Sale," "sell," or "sold" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale" does not include the following: (i) The disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer; (iii) the disclosure or transfer of personal data to an affiliate of the controller; (iv) the disclosure of information that the consumer (A) intentionally made available to the general public via a channel of mass media, and (B) did not restrict to a specific audience; or (v) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.	"Sale," "sell," or "sold" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating personal data, orally, in writing, or by electronic means, for monetary or other valuable consideration, or otherwise for a commercial purpose by a controller to a third party. "Sale" does not include the following: (i) The processing of personal data by a processor who processes the personal data on behalf of the controller pursuant to a contract; (ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer; (iii) the disclosure or transfer of personal data to an affiliate of the controller; (iv) the disclosure of information that the consumer (A) intentionally made available to the general public via a channel of mass media, and (B) did not restrict to a specific audience; or (v) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.	*Sec. 4(1)(b)* A legal entity is subject to the obligations in this act if it derives over 50% of gross revenue from the sale of personal data and processes or controls personal data of at least 25,000 consumers. *Sec. 4(2)* "Sale" is used in several exemptions. *Sec. 6(5)* A consumer has the right to opt out of the sale of personal data. *Sec. 8(1)* Controllers must clearly disclose whether they sell personal data to third parties. *Sec. 8(6)* A controller may not sell personal data obtained through a loyalty program, unless specified conditions are met. *Sec. 9(1)* Controllers must conduct and document a data protection assessment for each processing activity related to the sale of personal data.

PRIVACY COMPARISON: 2SSB 6281 and SHB 2742

Jurisdictional Scope *Section 4*	**2SSB 6281**	**SBH 2742**
To whom obligations apply	Legal entities that conduct business in Washington or produce products or services that are targeted to residents of Washington, and that satisfy one or more of the following thresholds: (a) During a calendar year, controls or processes personal data of 100,000 consumers or more; or (b) Derives over 50% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more.	Legal entities that conduct business in Washington or produce products or services that are targeted to residents of Washington.
Exempt entities	(a) State agencies, local governments, or tribes; (b) Municipal corporations;	(a) State and local governments; (b) Municipal corporations; (c) Legal entities that: (i) Have fewer than 10 employees; (ii) Have gross annual revenues of less than $5 million; (iii) Derive less than 5% of annual gross revenues from the sale or monetization of personal data at fair market value; (iv) Control or process personal data of fewer than 20,000 consumers; AND (v) Do not disclose or share personal data of consumers other than: (A) As necessary for providing products or services requested by consumers; or (B) For purposes of selling or monetizing personal data within the limits set in (c)(iii) of this subsection.
Exempt information	Personal data subject to enumerated federal and state laws, such as HIPAA, FCRA, GLBA, and the Farm Credit Act. Certain information is exempt only to the extent that its collection or processing is in compliance with the federal or state law to which the information is subject.	Personal data subject to enumerated federal and state laws, such as HIPAA, FCRA, GLBA, and the Farm Credit Act. Certain information is exempt only to the extent that its collection or processing is in substantial compliance with the federal or state law to which the information is subject.

Exempt information (cont'd)	Data maintained for employment record purposes is exempt. Institutions of higher education and nonprofit corporations are exempt until July 31, 2024.	Data maintained for employment record purposes is exempt until July 31, 2022.
Other jurisdictional provisions	Controllers that are in compliance with the verifiable parental consent mechanisms under the Children's Online Privacy Protection Act (COPPA) shall be deemed compliant with any obligation to obtain parental consent under this chapter	n/a

Responsibility according to role *Section 5*	**2SSB 6281**	**SHB 2742**
Responsibility according to role	Controllers and processors are responsible for meeting their respective obligations. Whether an entity is a processor or a controller with respect to specific processing of personal data is a fact-based determination. Processing by a processor is governed by a contract between the controller and the processor that sets out the processing instructions and other specified requirements. Processors are responsible for adhering to the instructions of the controller and assisting the controller in meeting its obligations. Processors must also implement and maintain reasonable security procedures to protect personal data, ensure confidentiality of the processing, and engage subcontractors only after certain requirements are met.	

PRIVACY COMPARISON: 2SSB 6281 and SHB 2742

<table>
<tr><th>Consumer rights
<em>Section 6</em></th><th>2SSB 6281</th><th>SHB 2742</th></tr>
<tr><td><strong>Consumer rights generally</strong></td><td>In the case of processing personal data concerning a known child, the parent or legal guardian of the known child shall exercise the rights of this chapter on the child's behalf.</td><td>Where a controller processes personal data concerning a known child, the controller must allow the parent or legal guardian of the known child to exercise the rights of this chapter on the child's behalf.
Where a controller processes personal data concerning a consumer subject to guardianship, conservatorship, or other protective arrangement under chapter 11.130 RCW, the controller must allow the guardian or the conservator to exercise the rights of this chapter on the consumer's behalf.</td></tr>
<tr><td><strong>Consumer rights and pseudonymous data</strong></td><td colspan="2">The rights of access, correction, deletion, and data portability do not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical, contractual, and organizational controls that prevent the controller from accessing such information.</td></tr>
<tr><td><strong>Right of access</strong></td><td colspan="2">A consumer has the right to confirm whether or not a controller is processing personal data concerning the consumer and access such personal data.</td></tr>
<tr><td><strong>Right to correction</strong></td><td>A consumer has the right to correct inaccurate personal data concerning the consumer, taking into account the nature of the personal data and the purposes of the processing of the personal data.</td><td>A consumer has the right to correct inaccurate personal data concerning the consumer.</td></tr>
<tr><td><strong>Right to deletion</strong></td><td colspan="2">A consumer has the right to delete personal data concerning the consumer.</td></tr>
<tr><td><strong>Right to data portability</strong></td><td colspan="2">A consumer has the right to obtain personal data concerning the consumer, which the consumer previously provided to the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.</td></tr>
<tr><td><strong>Right to opt out</strong></td><td>A consumer has the right to opt out of the processing of personal data concerning such consumer for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer.</td><td>A consumer has the right to opt out of the processing of personal data concerning such consumer.</td></tr>
</table>

Responding to consumer requests	A controller must inform a consumer of any action taken on a request without undue delay and in any event within 45 days of receipt of the request. That period may be extended once by 45 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 45 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 45 days of receipt of the request of the reasons for not taking action and instructions for how to appeal the decision with the controller.	A controller must inform a consumer of any action taken on a request without undue delay and in any event within 21 days of receipt of the request. That period may be extended once by 45 additional days where necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any such extension within 21 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 21 days of receipt of the request of the reasons for not taking action and instructions for how to appeal the decision with the controller.
Authenticating a consumer request	A controller is not required to comply with a request to exercise any of the rights [other than the right to opt out] if the controller is unable to authenticate the request using commercially reasonable efforts. In such cases, the controller may request the provision of additional information reasonably necessary to authenticate the request.	A controller is not required to comply with a request to exercise any of the rights [other than the right to opt out] if the controller is unable to authenticate the request. In such cases, the controller may request the provision of additional information necessary to authenticate the request.
Charging a fee to fulfill a consumer request	Information provided under this section must be provided by the controller free of charge, up to twice annually 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 to cover the administrative costs of complying with the request, or (ii) Refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.	

Notifying third parties of consumer requests	n/a	A controller must take reasonable steps to communicate a consumer's request to correct, delete, or opt out of the processing of personal data to each third party to whom the controller disclosed, including through sale, the personal data within one year preceding the consumer's request, unless this proves functionally impractical, technically infeasible, or involves disproportionate effort.
Internal appeal process	Controllers must establish an internal process whereby consumers may appeal a refusal to take action on a request to exercise any of the rights within a reasonable period of time after the consumer's receipt of the notice sent by the controller.	Controllers must establish an internal process whereby consumers may appeal a refusal to take action on a request to exercise any of the rights within 45 days of the consumer's receipt of the notice sent by the controller.
	The appeal process must be conspicuously available and as easy to use as the process for consumer rights requests. Within 30 days of receipt of an appeal, a controller must inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support thereof. That period may be extended by 60 additional days where necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The controller must inform the consumer of any such extension within 30 days of receipt of the appeal, together with the reasons for the delay. The controller must also provide the consumer with an email address or other online mechanism through which the consumer may submit the appeal, along with any action taken or not taken by the controller in response to the appeal and the controller's written explanation of the reasons in support thereof, to the Attorney General. When informing a consumer of any action taken or not taken in response to an appeal, the controller must clearly and prominently ask the consumer whether the consumer consents to having the controller submit the appeal, along with any action taken or not taken by the controller in response to the appeal and must, upon request, provide the controller's written explanation of the reasons in support thereof, to the Attorney General. If the consumer provides such consent, the controller must submit such information to the Attorney General.	

Responsibilities of Controllers and Processors *Sections 7 - 9*	**2SSB 6281**	**SHB 2742**
Transparency	Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes: (i) The categories of personal data processed by the controller; (ii) The purposes for which the categories of personal data are processed; (iii) How and where consumers may exercise the rights, including how a consumer may appeal a controller's action with regard to the consumer's request; (iv) The categories of personal data that the controller shares with third parties, if any; and (v) The categories of third parties, if any, with whom the controller shares personal data. If a controller sells personal data to third parties or processes personal data for targeted advertising, it must clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing, in a clear and conspicuous manner. Controllers shall establish, and shall describe in the privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their rights under this chapter. Such means shall take into account the ways in which consumers interact with the controller, the need for secure and reliable communication of such requests, and the controller's ability to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise a right, but a controller may require a consumer to use an existing account to exercise the consumer's rights under this chapter.	
Purpose specification	A controller's collection of personal data must be limited to what is reasonably necessary in relation to the purposes for which such data are processed, as disclosed to the consumer.	
Data minimization	A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the purposes for which such data are processed, as disclosed to the consumer.	A controller's collection of personal data must be only as reasonably necessary to provide services requested by a consumer, to conduct an activity that a consumer has requested, or to verify [consumer rights] requests.
Avoid secondary use	Except as provided in this chapter, a controller may not process personal data for purposes that are not reasonably necessary to, or compatible with, the purposes for which such personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.	

Security	A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue.	
Nondiscrimination and responsibilities related to loyalty programs	A controller may not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. This subsection shall not prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program. A controller may not sell personal data to a third-party controller as part of such a program unless: (a) The sale is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled; (b) the sale of personal data to third parties is clearly disclosed in the terms of the program; and (c) the third party uses the personal data only for purposes of facilitating such benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.	
	A controller may not enroll a consumer in a facial recognition service in connection with a bona fide loyalty, rewards, premium features, discounts, or club card program.	n/a
Processing sensitive data	Except as otherwise provided in this act, a controller may not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of personal data concerning a known child, without obtaining consent from the child's parent or lawful guardian, in accordance with the COPPA requirements.	Except as otherwise provided in this act, a controller may not process sensitive data concerning a consumer without obtaining the consumer's consent. Except as otherwise provided in this act, a controller may not process sensitive data of a known child without obtaining consent from the child's parent or lawful guardian.
Nonwaiver of consumer rights	Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this chapter shall be deemed contrary to public policy and shall be void and unenforceable.	
Using deidentified or pseudonymous data	A controller that uses pseudonymous data or deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data are subject, and must take appropriate steps to address any breaches of contractual commitments.	

<table>
<tr>
<td rowspan="2"><b>Conducting data protection assessments</b></td>
<td colspan="2"><b>Controllers must conduct and document a data protection assessment of each of the following processing activities involving personal data:</b>

(a) The processing of personal data for purposes of targeted advertising;
(b) The sale of personal data;
(c) The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of:
(i) Unfair or deceptive treatment of, or disparate impact on, consumers;
(ii) Financial, physical, or reputational injury to consumers;
(iii) Physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or
(iv) Other substantial injury to consumers;
(d) The processing of sensitive data; and
(e) Any processing activities involving personal data that present a heightened risk of harm to consumers.

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

Data protection assessments must identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks.

The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, must be factored into this assessment by the controller.

The Attorney General may evaluate the data protection assessments for compliance with the responsibilities [of the controllers and processors] and with other laws including, but not limited to, chapter 19.86 RCW.

Data protection assessments are confidential and exempt from public inspection and copying under chapter 42.56 RCW.

Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may qualify under this section if they have a similar scope and effect</td>
</tr>
<tr>
<td>The Attorney General may request, in writing, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General.</td>
<td>The Attorney General may request, in writing, that a controller disclose any data protection assessment that is relevant to an investigation of the controller conducted by the Attorney General.</td>
</tr>
</table>

PRIVACY COMPARISON: 2SSB 6281 and SHB 2742

Limitations to the responsibilities of controllers and processors	**2SSB 6281**	**SHB 2742**
Limitations to the responsibilities of controllers and processors ***Sec. 7***	**This chapter does not require a controller or processor to do any of the following solely for purposes of complying with this chapter:** (a) Reidentify deidentified data;	
	(b) Comply with an authenticated consumer request to access, correct, delete, or port personal data, if all of the following are true: (i) (A) The controller is not reasonably capable of associating the request with the personal data, or (B) it would be unreasonably burdensome for the controller to associate the request with the personal data; (ii) The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and (iii) The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section; or	(b) Comply with an authenticated consumer request to access, correct, delete, or port personal data, if all of the following are true: (i) (A) The controller is not capable of associating the request with the personal data, or (B) it would be unusually burdensome for the controller to associate the request with the personal data; (ii) The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and (iii) The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section; or
	(c) Maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.	
Limitations to the responsibilities of controllers and processors ***Sec. 10***	**The obligations imposed on controllers or processors 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 laws, rules, or regulations; (d) Investigate, establish, exercise, prepare for, or defend legal claims; (e) Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;	

Limitations to the responsibilities of controllers and processors ***Sec. 10*** (cont'd)	**The obligations imposed on controllers or processors do not restrict a controller's or processor's ability to:**	
	(f) Take immediate steps to protect an interest that is essential for the life of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;	(f) Protect the vital interests of the consumer or of another natural person;
	(g) Prevent, detect, protect against, 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;	
	(h) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws if the deletion of the information is likely to render impossible or seriously impair the achievement of the research and the consumer provided consent; or	(h) Process personal data to conduct ongoing scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or a similar independent oversight entity that determines that: (i) The research is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) The expected benefits of the research outweigh the privacy risks; and (iii) The controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or
	(i) Assist another controller, processor, or third party with any of the obligations under this subsection.	
	The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to collect, use, or retain data to:	
	(a) Conduct internal research solely to improve or repair products, services, or technology;	(a) Conduct internal research to improve, repair, or develop products, services, or technology;
	(b) Identify and repair technical errors that impair existing or intended functionality; or	
	(c) Perform solely internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with processing in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.	(c) Perform internal operations that are aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with processing in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

<table>
<tr><td rowspan="3"><b>Requirements for processing pursuant to an exemption in Sec. 10</b></td><td colspan="2">Personal data that are processed by a controller pursuant to this section must not be processed for any purpose other than those expressly listed in this section.</td></tr>
<tr><td>Personal data that are processed by a controller pursuant to this section may be processed solely to the extent that such processing is:
(i) Necessary, reasonable, and proportionate to the purposes listed in this section; and
(ii) Adequate, relevant, and limited to what is necessary in relation to the specific purpose or purposes listed in this section.
Furthermore, personal data that are collected, used, or retained pursuant to this section must, insofar as possible, taking into account the nature and purpose or purposes of such collection, use, or retention, be subjected to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data, and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.</td><td>Personal data that are processed by a controller pursuant to this section may be processed solely to the extent that such processing is:
(i) Necessary and proportionate to the purposes listed in this section; and
(ii) Adequate, relevant, and limited to what is necessary in relation to the specific purpose or purposes listed in this section.
Furthermore, personal data that are collected, used, or retained pursuant to this section must be subjected to administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data, and to reduce foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.</td></tr>
<tr><td colspan="2">If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection (6) of this section.</td></tr>
</table>

PRIVACY COMPARISON: 2SSB 6281 and SHB 2742

Commercial use of facial recognition services	2SSB 6281 *Section 17*	SHB 2742 *Section 16*
Testing for accuracy and unfair performance differences	Processors that provide facial recognition services must make available an application programming interface or other technical capability, chosen by the processor, to enable controllers or third parties to conduct legitimate, independent, and reasonable tests of those facial recognition services for accuracy and unfair performance differences across distinct subpopulations: PROVIDED, That making such an application programming interface or other technical capability available does not require the disclosure of proprietary data, trade secrets, intellectual property, or other information, or if doing so would increase the risk of cyberattacks including, without limitation, cyberattacks related to unique methods of conducting business, data unique to the product or services, or determining prices or rates to be charged for services.	Prior to deploying a facial recognition service, processors that provide facial recognition services must make available an application programming interface or other technical capability, chosen by the processor, to enable controllers or third parties to conduct legitimate, independent, and reasonable tests of those facial recognition services for accuracy and unfair performance differences across distinct subpopulations.
	Such subpopulations are defined by visually detectable characteristics, such as (a) race, skin tone, ethnicity, gender, age, or disability status, or (b) other protected characteristics that are objectively determinable or self-identified by the individuals portrayed in the testing dataset.	Such subpopulations are defined by visually detectable characteristics, such as (a) race, skin tone, ethnicity, gender, age, or disability status, or (b) other protected characteristics that are objectively determinable or self-identified by the individuals portrayed in the testing dataset.
	If the results of that independent testing identify material unfair performance differences across subpopulations and the methodology, data, and results are disclosed in a manner that allow full reproduction of the testing directly to the processor, who, acting reasonably, determines that the methodology and results of that testing are valid, then the processor must develop and implement a plan to mitigate the identified performance differences.	If the results of that independent testing identify material unfair performance differences across subpopulations and the methodology, data, and results are disclosed in a manner that allow full reproduction of the testing directly to the processor, who determines that the methodology and results of that testing are valid, then the processor must develop and implement a plan to mitigate the identified performance differences.
	Nothing in this subsection prevents a processor from prohibiting the use of the processor's facial recognition service by a competitor for competitive purposes.	Nothing in this subsection prevents a processor from prohibiting the use of the processor's facial recognition service by a competitor for competitive purposes.

Providing documentation about FR	Processors that provide facial recognition services must provide documentation that includes general information that: (a) Explains the capabilities and limitations of the services in plain language; and (b) Enables testing of the services in accordance with this section.	
Prohibiting the use of FR to unlawfully discriminate	Processors that provide facial recognition services must prohibit the use of facial recognition services by controllers to unlawfully discriminate under federal or state law against individual consumers or groups of consumers.	
Providing notice of the use of FR	Controllers must provide a conspicuous and contextually appropriate notice whenever a facial recognition service is deployed in a physical premise open to the public that includes, at minimum, the following: (a) The purpose or purposes for which the facial recognition service is deployed; and (b) Information about where consumers can obtain additional information about the facial recognition service including, but not limited to, a link to any applicable online notice, terms, or policy that provides information about where and how consumers can exercise any rights that they have with respect to the facial recognition service.	Controllers must provide a conspicuous and contextually appropriate notice whenever a facial recognition service is deployed including, at minimum, the following: (a) The purpose or purposes for which the facial recognition service is deployed; (b) Notification that controllers must obtain a consumer's consent prior to enrolling an image of that consumer in a facial recognition service and that consent is not required in order to obtain entry to a physical place open to the public, or to be provided with goods or services without discrimination or penalty for not consenting; and (c) Information about where consumers can obtain additional information about the facial recognition service including, but not limited to, a link to any applicable online notice, terms, or policy that provides information about where and how consumers can exercise any rights that they have with respect to the facial recognition service.
Obtaining consumer consent prior to enrolling an image	Controllers must obtain consent from a consumer prior to enrolling an image of that consumer in a facial recognition service used in a physical premise open to the public.	Controllers must obtain consent from a consumer prior to enrolling an image of that consumer in a facial recognition service. Controllers may not deny goods or services, deny entry to a physical place open to the public, or otherwise discriminate against or penalize a consumer who does not consent to enrollment of the consumer's image in a facial recognition service.

Enrolling an image without consent	**Controllers may enroll an image of a consumer in a facial recognition service for a security or safety purpose without first obtaining consent from that consumer, provided that all the following requirements are met:** (a) The controller must hold a reasonable suspicion, based on a specific incident, that the consumer has engaged in criminal activity, which includes, but is not limited to, shoplifting, fraud, stalking, or domestic violence; (b) Any database used by a facial recognition service for identification, verification, or persistent tracking of consumers for a security or safety purpose must be used solely for that purpose and maintained separately from any other databases maintained by the controller; (c) The controller must review any such database used by the controller's facial recognition service no less than annually to remove facial templates of consumers whom the controller no longer holds a reasonable suspicion that they have engaged in criminal activity; and (d) The controller must establish an internal process whereby a consumer may correct or challenge the decision to enroll the image of the consumer in a facial recognition service for a security or safety purpose.	
Notice of image used for verification	n/a	Controllers that use a facial recognition service for verification purposes must provide the consumer with notice as to which image of the consumer the facial recognition service is referencing when attempting to verify the consumer's identity.
Meaningful human review	Controllers using a facial recognition service to make decisions that produce legal effects on consumers or similarly significant effects on consumers must ensure that those decisions are subject to meaningful human review.	Controllers using a facial recognition service for the purpose of verification, identification, or to make decisions that produce legal effects on consumers or similarly significant effects on consumers must ensure that those decisions are subject to meaningful human review.
Testing in operational conditions	Prior to deploying a facial recognition service in the context in which it will be used, controllers using a facial recognition service to make decisions that produce legal effects on consumers or similarly significant effects on consumers must test the facial recognition service in operational conditions.	
Ensuring best quality results	Controllers must take commercially reasonable steps to ensure best quality results by following all reasonable guidance provided by the developer of the facial recognition service.	Controllers must take steps to ensure best quality results by following all guidance provided by the developer of the facial recognition service.
Training	Controllers using a facial recognition service must conduct periodic training of all individuals that operate a facial recognition service or that process personal data obtained from the use of facial recognition services.	Controllers using a facial recognition service must conduct annual training of all individuals that operate a facial recognition service or that process personal data obtained from the use of facial recognition services.

Training ***(cont'd)***	Such training shall include, but not be limited to, coverage of: (a) The capabilities and limitations of the facial recognition service; (b) Procedures to interpret and act on the output of the facial recognition service; and (c) The meaningful human review requirement for decisions that produce legal effects on consumers or similarly significant effects on consumers, to the extent applicable to the deployment context.	Such training shall include, but not be limited to, coverage of: (a) The capabilities and limitations of the facial recognition service; (b) Procedures to interpret and act on the output of the facial recognition service; and (c) The meaningful human review requirement for verification, identification, or decisions that produce legal effects on consumers or similarly significant effects on consumers, to the extent applicable to the deployment context.
Disclosing personal data obtained from FR	Controllers shall not knowingly disclose personal data obtained from a facial recognition service to a law enforcement agency, except when such disclosure is:	Controllers shall not disclose personal data obtained from a facial recognition service to a law enforcement agency, except when such disclosure is:
	(a) Pursuant to the consent of the consumer to whom the personal data relates; (b) Required by federal, state, or local law in response to a court order, court-ordered warrant, or subpoena or summons issued by a judicial officer or grand jury; (c) Necessary to prevent or respond to an emergency involving danger of death or serious physical injury to any person, upon a good faith belief by the controller; or (d) To the national center for missing and exploited children.	
Facial recognition data as evidence	n/a	No information obtained from or by the use of a facial recognition service may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority subject to the jurisdiction of the state of Washington.
Complying with other responsibilities	Controllers that deploy a facial recognition service must respond to a consumer request to exercise the rights and fulfill the [controller] responsibilities.	
Exemption for verification of aviation passengers	Voluntary facial recognition services used to verify an aviation passenger's identity are exempt. Images captured by an airline must not be retained for more than 24 hours and, upon request of the Attorney General, airlines must certify that they do not retain the image for more than twenty-four hours. An airline facial recognition service must disclose and obtain consent from the customer prior to capturing an image.	

Preemption	2SSB 6281	SHB 2742
Preemption of local regulations	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.	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. This chapter does not supersede or preempt laws, ordinances, regulations, or the equivalent adopted by any local entity regarding facial recognition.

Liability and Enforcement	2SSB 6281	SHB 2742
Liability	Any violation of this chapter shall not serve as the basis for, or be subject to, a private right of action under this chapter or under any other law. This does not relieve any party from any duties or obligations imposed, or to alter any independent rights that consumers have under other laws, chapter 19.86 RCW, the Washington state Constitution, or the United States Constitution. 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 must be allocated among the parties according to principles of comparative fault.	n/a
Enforcement and penalties	The Attorney General has exclusive authority to enforce this chapter by bringing an action in the name of the state, or as parens patriae on behalf of persons residing in the state. Any controller or processor that violates this chapter is subject to an injunction and liable for a civil penalty of not more than $7,500 for each violation.	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. Any controller or processor that violates this chapter is subject to an injunction and liable for a civil penalty of not more than $50,000 for each violation or $100,000 for each intentional violation.

PRIVACY COMPARISON: 2SSB 6281 and SHB 2742

<table>
<tr><th>Reports and Research Initiatives</th><th>2SSB 6281</th><th>SHB 2742</th></tr>
<tr><td><b>Attorney General report</b></td><td colspan="2">The Attorney General shall compile a report evaluating the liability and enforcement provisions of this chapter including, but not limited to, the effectiveness of its efforts to enforce this chapter, and any recommendations for changes to such provisions.

The Attorney General shall submit the report to the governor and the appropriate committees of the legislature by July 1, 2022.</td></tr>
<tr><td><b>Joint research initiatives</b></td><td colspan="2">The governor may enter into agreements with the governments of the Canadian province of British Columbia and the states of California and Oregon for the purpose of sharing personal data or personal information by public bodies across national and state borders to enable collaboration for joint data-driven research initiatives. Such agreements must provide reciprocal protections that the respective governments agree appropriately safeguard the data.</td></tr>
</table>