Provides that this act shall be known as the Washington Privacy Act

Provides that the legislature finds that the people of Washington regard their privacy as a fundamental right and that Washington’s Constitution explicitly provides the right to privacy

Provides that this act:
  - Applies to legal entities that conduct business or produce products that are targeted to Washington residents and:
    - Control or process personal data of more than 100,000 consumers; or
    - Derive 50 percent of gross revenue from the sale of personal data and process or control the personal data of over 25,000 consumers;
  - Does not apply to state and local governments; municipal corporations; personal data governed by certain state and federal regulations; and employment records

Provides that a consumer may exercise the following rights regarding their personal data:
  - Access: Confirmation if a controller is processing their data and access to that data
  - Correction: Correct inaccurate data
  - Deletion: Delete personal data
  - Data Portability: Obtain personal data in a portable format to transmit to another entity
  - Opt-out: Opt-out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, and profiling in furtherance of decisions that produce legal effects

Provides that a controller or processor is not required to take certain steps in order to comply with this act, such as identifying deidentified data or maintaining data in an identified form

Requires controllers that use deidentified or pseudonymous data to exercise reasonable oversight and take steps to address contractual commitments

Specifies controller responsibilities, including:
  - Transparency: Provide a privacy notice that meets certain requirements, including telling consumers how they can exercise their rights
  - Purpose Specification: Limit collection of data to what is required for a specified purpose
  - Data Minimization: Limit collection of data to what is relevant to a specified purpose
  - Secondary Use: Prohibit processing for purposes not compatible with a specified purpose
  - Care: Secure personal data from unauthorized acquisition
  - Non-Discrimination: Prohibit processing which violates state or federal law and discriminating against a consumer for exercising any of the consumer rights of this act
  - Sensitive Data: Obtain consumer consent in order to process sensitive data
• Requires controllers to conduct a data protection assessment for each of their processing activities involving personal data and an additional data protection assessment any time there is a change in processing that materially increases the risk to consumers

• Authorizes the Attorney General to request a data protection assessment relevant to an investigation

• Specifies limitations for when the obligations imposed on controllers or processors under this chapter do restrict a controller or processor, such as complying with federal, state, or local laws

• Requires controllers or processors that process data pursuant to an exemption to demonstrate that the processing qualifies for an exemption and ensure that processing is limited to that specified purpose; processing must be proportionate to the specified purpose

• Provides that any violation of this chapter does not serve as the basis for a private right of action under this act or any other law

• Authorizes the Attorney General to bring an action and prescribes a penalty of not more than $7,500 for each violation

• Requires the Attorney General to submit a report by July 1, 2022 evaluating the liability and enforcement provisions of this act and provide recommendations for any changes

• Requires the state Office of Privacy and Data Protection to conduct a study on the development of global-opt out technologies and submit a report of findings and recommendations to the Legislature by Oct. 31, 2021

• Authorizes the governor to enter into agreements with British Columbia, California, and Oregon for the purpose of sharing personal data for joint research initiatives

• Provides a regulatory framework for the commercial use of facial recognition services by controllers and processors, which includes:
  o Third-party testing of the technology for accuracy and unfair performance
  o Testing of the technology in operational conditions prior to deployment
  o Consumer consent prior to enrolling an image in a service used in a public space
  o Conspicuous notice where the technology is deployed in a public space
  o Periodic training for all technology operators

• Provides on effective date of July 31, 2021; Office of Privacy and Data Protection study effective 90 days after enactment