Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Civil Rights & Judiciary Committee

HB 1850

Brief Description: Protecting and enforcing the foundational data privacy rights of Washingtonians.

Sponsors: Representatives Slatter, Berg, Pollet and Harris-Talley.

Brief Summary of Bill

- Establishes consumer personal data rights of access, correction, deletion, data portability, and opt-out of the processing of personal data for specified purposes.
- Defines obligations for controllers and processors of personal data who are legal entities that meet specified thresholds.
- Identifies controller responsibilities, including transparency, purpose specification, data minimization, security, and nondiscrimination.
- Exempts state and local government, tribes, air carriers, employment-related data, certain nonprofit organizations, and data sets subject to regulation by specified federal and state laws.
- Creates the Washington State Consumer Data Privacy Commission vested with administrative, rulemaking, and enforcement authority.
- Provides that violations are enforceable by the Attorney General under the Consumer Protection Act and subject to civil penalties.
- Creates a private right of action to enjoin violations and recover actual damages.
- Imposes an annual fee on data collectors.

Hearing Date: 1/25/22

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not part of the legislation nor does it constitute a statement of legislative intent.

Staff: Yelena Baker (786-7301).

Background:

Federal Laws Related to Privacy.
A sectorial framework protects personal information and privacy interests under various federal laws. Key federal statutes related to privacy include:

- the Health Insurance Portability and Accountability Act, which protects the privacy and security of medical information;
- the Fair Credit Reporting Act, which regulates the consumer reporting industry and provides privacy rights in consumer reports;
- the Gramm-Leach-Bliley Act, which regulates the sharing of personally identifiable financial information by financial institutions and their affiliates; and
- the Family Educational Rights and Privacy Act, which protects the privacy of student education records.

Comprehensive Privacy Laws in Other States.
While no single general privacy law exists at the federal level, three states have recently enacted comprehensive data privacy laws that regulate the collection and sharing of personal information.

The California Consumer Privacy Act (CCPA) took effect in 2020 and regulates the collection, use, and sharing of personal information. The CCPA provides California residents with certain data rights, such as the right to access or delete collected personal information and to opt out of the sale of personal information to third parties, and specifies obligations of businesses that collect and process consumers' personal information.

In November 2020 California residents approved a ballot initiative titled the California Privacy Rights Act (CPRA), which amends and expands the CCPA and establishes a new enforcement agency dedicated to consumer privacy. The CPRA takes effect January 1, 2023.

Signed into law in early March 2021, the Virginia Consumer Data Protection Act (VCDPA) regulates the collection and use of consumer personal data and grants Virginia residents the rights to access, correct, delete, and opt out of the sale and processing of their personal data for targeted advertising purposes. Under the VCDPA, controllers and processors that collect and use consumers' personal data have obligations of data minimization, purpose limitation, and reasonable data security. The state Attorney General has investigative authority and exclusive authority to enforce violations of the VCDPA. The VCDPA goes into effect January 1, 2023.

Largely following the VCDPA framework, the Colorado Privacy Act grants consumer personal data rights, specifies obligations of controllers and processors that process personal data, and gives the state Attorney General and district attorneys exclusive enforcement authority under the Colorado Consumer Protection Act. The Colorado Privacy Act takes effect July 1, 2023.

Privacy Protection in Washington.
The Washington Constitution provides that no person shall be disturbed in their private affairs without authority of law. As with the federal sectorial approach, different state statutes define permitted conduct and specify the requisite level of privacy protections for medical records, financial transactions, student information, biometric identifiers, and other personal data.

Washington Consumer Protection Act.
The Consumer Protection Act (CPA) prohibits unfair methods of competition or unfair or deceptive practices in the conduct of any trade or commerce. The Attorney General is authorized to investigate and prosecute claims under the CPA on behalf of the state or individuals in the state. A person injured by a violation of the CPA may bring a civil action for injunctive relief, recovery of actual damages, and reasonable attorneys' fees. The courts may increase awarded damages up to three times the actual damages sustained.

Summary of Bill:

Key Definitions.
"Consumer" means a natural person who is a Washington resident acting only in an individual or household context. "Consumer" does not include a natural person acting in a commercial or employment context.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person, household, or consumer device. "Personal data" includes pseudonymous data but does not include deidentified data or publicly available information.

Jurisdictional Scope.
The Washington Foundational Data Privacy Act (FDPA) applies to controllers and processors who are legal entities that conduct business in Washington or produce products or services that are targeted to Washington residents and meet the following thresholds:

- control or process personal data of 100,000 or more consumers during a calendar year; or
- control or process personal data of 25,000 or more consumers and derive over 25 percent of gross revenue from the sharing of personal data.

For purposes of these thresholds, "consumer" does not include payment-only transactions where no data about consumers are retained.

The FDPA does not apply to:

- state agencies, legislative agencies, the judicial branch, local governments, municipal corporations, or tribes;
- air carriers;
- nonprofit organizations that are registered with the Secretary of State under the Charities Program, collect personal data during legitimate activities related to the organization's tax-exempt purpose, and do not share personal data;
- data maintained in specified employment-related contexts;

- personal data collected, maintained, disclosed, or otherwise used in connection with the gathering, dissemination, or reporting of news or information to the public by news media; and
- information subject to enumerated federal and state laws.

Certain personal data are exempt only to the extent that the collection or processing of that data is in compliance with federal and state laws to which the data are subject and which are specified in the exemptions.

Institutions of higher education and nonprofit corporations are exempt until July 31, 2027.

Consent Requirement.
Controllers may not process:
- personal data for purposes that are not reasonably necessary to or compatible with the purposes for which the data are processed unless pursuant to consumer consent;
- personal data of a minor for the purposes of targeted advertising or sharing of personal data without obtaining the minor's consent; or
- sensitive data without consumer consent.

Controllers must provide an effective mechanism for a consumer to revoke consent. After a consumer revokes consent, the controller must cease processing the consumer's sensitive data as soon as practicable, but no later than 15 days after revocation.

Consumer Rights Concerning Personal Data.
With regard to the processing of personal data, a consumer has the following rights:
- confirm whether a controller is processing the consumer's personal data;
- access the personal data being processed by the controller;
- correct inaccurate personal data, taking into account the nature of the personal data and the purposes of processing;
- delete personal data;
- obtain in a portable format the consumer's personal data previously provided to the controller; and
- opt out of the processing for purposes of targeted advertising, the sharing of personal data, or profiling in furtherance of decisions that produce legal effects or similarly significant effects on the consumer.

Except for the right to opt out, the consumer personal data rights do not apply to pseudonymous data where the controller is able to demonstrate that 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.

Exercising Consumer Personal Data Rights.
A consumer or a consumer's authorized agent may exercise personal data rights by submitting to a controller a request that specifies which rights the consumer wishes to exercise.

The parent or legal guardian of a known child may exercise consumer personal data rights on the child's behalf. If a controller processes personal data of a consumer subject to guardianship, conservatorship, or other protective arrangement, the guardian or conservator may exercise consumer personal data rights on behalf of the consumer.

A consumer may exercise the right to opt out of the processing for purposes of targeted advertising or sharing of personal data:

- by designating an authorized agent who may exercise the rights on behalf of the consumer; or
- via user-enabled global privacy controls, such as a browser plug-in or privacy setting or device setting, that communicates the consumer's choice to opt out.

Responding to Consumer Requests to Exercise Personal Data Rights.
A controller is not required to comply with a consumer personal data right request if the controller is unable to authenticate the request using commercially reasonable efforts. The authentication requirement does not apply to the right to opt out.

A controller must comply with the request to exercise the right to opt out as soon as feasible, but no later than within 15 days of receiving the request. A controller must inform the consumer of any action taken on requests to access, correct, delete, or obtain a copy of the consumer's personal data within 45 days of receiving the request. This period may be extended once by 45 additional days where reasonably necessary, provided that the controller informs the consumer of the extension and the reasons for the delay within the first 45-day period.

If a controller does not take action on a request, the controller must inform the consumer within 45 days of receiving the request and provide reasons for not taking action, as well as instructions on how to appeal the decision with the controller.

Controllers must establish an internal process by which a consumer may appeal a refusal to take action on the consumer's personal data right requests. Within 30 days of receiving an appeal, the controller must inform the consumer of action taken or not taken in response to the appeal and provide a supporting written explanation. This period may be extended by 60 additional days, provided that the controller informs the consumer of the extension and the reasons for the delay within the initial 30-day period.

When informing a consumer of any action taken or not taken in response to an appeal, the controller must clearly and prominently provide the consumer with information about how to file a complaint with the Washington State Consumer Data Privacy Commission. In addition, controllers must provide consumers with an electronic mail address or other online mechanism through which the consumers may submit the results of an appeal and supporting documentation to the Attorney General.

A controller must maintain records of all appeals and the controller's responses to appeals for at

least 24 months and must compile and provide a copy of appeal records to the Attorney General upon request.

Information provided to a consumer pursuant to a personal data right request must be provided free of charge, up to twice annually. If a request from a consumer is manifestly unfounded or excessive, the controller may charge a reasonable fee or refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive nature of the request.

Responsibilities of Controllers and Processors.
Controllers must:

- provide consumers with a clear and meaningful privacy notice that meets certain requirements (transparency);
- limit the collection of personal data to what is reasonably necessary, in relation to the purposes for which the data are processed (purpose specification);
- collect personal data in a manner that is adequate, relevant, and limited to what is reasonably necessary, in relation to the purpose for which the data are processed (data minimization); and
- implement and maintain reasonable data security practices (data security).

A controller or processor that uses deidentified or pseudonymous data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified or pseudonymous data are subject.

Processors are responsible for adhering to the processing instructions and assisting controllers in meeting their obligations. In addition, processors must implement and maintain reasonable security procedures to protect personal data and ensure confidentiality of processing and may engage subcontractors only after specified requirements are met.

Nondiscrimination and Nonretaliation.
Controllers may not process personal data on the basis of a consumer's protected characteristic in a manner that unlawfully discriminates against the consumer.

Controllers may not retaliate against a consumer for exercising consumer rights, including by charging different prices or rates for goods and services or providing a different quality of goods and services to the consumer. The nonretaliation requirement does not prohibit a controller from offering different prices or rates of service to a consumer who voluntarily participates in a bona fide loyalty or rewards program. If a consumer exercises the right to opt out, personal data collected as part of a loyalty or rewards program may not be shared with a third-party controller unless specified conditions are met.

Data Protection Assessments.
Controllers must conduct a data protection assessment of each of the following processing activities:

- processing for purposes of targeted advertising;
- sharing of personal data;
- processing for purposes of profiling, where such profiling presents a specified reasonably foreseeable risk;
- processing of sensitive data; and
- any processing that presents a heightened risk of harm to consumers.

Data protection assessments must identify and weigh the benefits of processing to a controller, consumer, other stakeholders, and the public against the risks to the rights of the consumer. Data protection assessments conducted for the purpose of complying with other laws may qualify if they have a similar scope and effect.

The Attorney General may request that a controller disclose any data protection assessment relevant to an investigation conducted by the Attorney General and evaluate the assessment for compliance with the controller responsibilities under this act and other laws, including the Consumer Protection Act. Data protection assessments disclosed to the Attorney General are confidential and exempt from public inspection.

Limitations to the Responsibilities of Controllers and Processors.
Controllers and processors are not required to do the following in order to comply with this act:

- reidentify deidentified data;
- comply with an authenticated consumer request to access, correct, delete, or obtain personal data in a portable format if specified circumstances exist; or
- maintain data in an identifiable form.

In addition, the obligations imposed on controllers or processors do not restrict their ability to take certain actions, including:

- comply with federal, state, or local laws, or with a civil, criminal, or regulatory inquiry, subpoena, or summons by federal, state, local or other governmental authorities;
- provide a product or service specifically requested by a consumer;
- take immediate steps to protect an interest that is essential for the life of a consumer or another natural person, where the processing cannot be manifestly based on another legal basis;
- protect against or respond to illegal activity;
- engage in public or peer-reviewed scientific, historical, or statistical research in the public interest, if specified conditions are met;
- collect, use, or retain data to conduct internal research solely to improve or repair products, services, or technology;
- collect, use, or retain data to identify and repair technical errors that impair existing or intended functionality; or
- perform solely internal operations that are reasonably aligned with the expectations of a consumer or are otherwise compatible with processing for purposes of performing a contract to which the consumer is a party.

To qualify for an exemption, the processing of a consumer's personal data must be reasonably necessary and proportionate for these purposes. The controller bears the burden of demonstrating that the processing qualifies for an exemption and complies with specified requirements. Personal data processed pursuant to an exemption may be processed solely to the extent that the processing is necessary, reasonable, and proportionate to the exempt purposes, and must not be processed for any other purposes.

Washington State Consumer Data Privacy Commission.
The Washington State Consumer Data Privacy Commission (Commission) is created and vested with full administrative power, authority, and jurisdiction to implement and enforce the FDPA and the rules adopted under the FDPA by the Commission.

The Commission is composed of three members to be appointed by the Governor with advice and consent of the Senate. One of the Commission members must be designated as chairperson by the Governor. The term of each commissioner is five years, with eligibility for reappointment.

The Washington Utilities and Transportation Commission must provide all administrative staff support for the Commission. The Commission may employ staff as necessary to carry out the Commission's duties. The Commission may appoint an executive director to perform the duties as prescribed by the Commission. With certain exceptions, the Commission may delegate to the executive director the powers to implement and enforce the FDPA efficiently and effectively.

Members of the Commission must:
- have qualifications, experience, and skills in the areas of privacy and technology;
- remain free from external influence;
- refrain from any action incompatible with their duties; and
- be precluded, for a period of one year after leaving office, from accepting employment with a controller or processor that was subject to an enforcement action or civil action during the member's tenure or during the five-year period preceding the member's appointment.

The Commission must perform specified functions, including:
- adopt suitable rules to carry out the purposes and provisions of the FDPA
- protect fundamental privacy rights of consumers with respect to the use of their personal data;
- promote public awareness and understanding of risks, safeguards, and rights in relation to the processing of personal data;
- monitor relevant developments related to the protection of personal data;
- provide technical assistance and advice to the Legislature;
- provide guidance, upon request, to controllers and processors regarding their obligations;
- establish a data protection certification mechanism; and
- conduct data protection audits of controllers and processors.

Annual Registration Requirement.
Controllers and processors must register annually with the Commission and provide certain information regarding their personal data processing operations, including:

- whether the controller or processor offers an opt-in or opt-out model for its personal data processing operations and how a consumer can access these options;
- a statement specifying the methods used for personal data processing operations and databases maintained; and
- a statement specifying the amount of personal data of Washington consumers collected, processed, or shared in the preceding year.

Upon registration, controllers and processors must pay a $250 or $450 registration fee, depending on the controller or processor's annual gross revenue in the year preceding registration.

A controller or processor that fails to register is subject to a fine between $1,000 and $20,000 for each day it fails to register. A controller or processor that knowingly submits false or incomplete information upon registration is subject to a fine between $10,000 and $100,000. All fines must be levied by the Commission. When determining the amount of fines to be levied, the Commission must consider factors such as the controller or processor's gross annual revenue and assets, and whether the controller or processor made reasonable efforts to comply with the registration requirements.

Administrative Enforcement by the Consumer Data Privacy Commission.
Upon the complaint of a consumer or on its own initiative, the Commission may investigate alleged violations by a controller or processor or refer the complaint to the Attorney General. Upon request by the Attorney General, the Commission must stay an administrative action or investigation to permit the Attorney General to proceed with an investigation or civil action.

Taking into consideration certain factors, such as the lack of intent to violate, the Commission may decide not to investigate a complaint or decide to provide a controller or processor with a time period to cure the alleged violation.

At least 30 days prior to the Commission's consideration of the alleged violation, the Commission must provide the alleged violator with a notice of the alleged violation and a summary of the evidence, and inform the alleged violator of the right to be present in person and presented by counsel at any proceeding by the Commission. A proceeding held for the purpose of considering whether there is reason to believe that a violation has occurred is private unless the alleged violator files with the Commission a written request that the proceeding be public.

If the Commission determines there is reason to believe that a violation occurred, the Commission must hold a hearing to determine if a violation has occurred. Notice must be given and the hearing conducted in accordance with the Administrative Procedure Act.

If the Commission determines that no violation has occurred, it must publish a declaration so

stating. If the Commission determines that a violation has occurred, the Commission shall issue an order that may require the violator to:

- cease and desist the violation; or
- pay an administrative fine of up to $2,500 for each violation, or up to $7,500 for each intentional violation and each violation involving a minor's personal data.

Any decision of the Commission is subject to judicial review.

Civil Enforcement by the Attorney General.
The Attorney General may enforce the FDPA under the Consumer Protection Act. No action may be filed by the Attorney General for any violation by a controller or processor after the Commission has issued a decision against that controller or processor for the same violation.

Until July 1, 2023, prior to filing a complaint, the Attorney General must provide the controller or processor with a warning letter identifying the alleged violations. If the controller or processor fails to cure any alleged violation within 30 days, the Attorney General may bring an action against the controller or processor.

Private Right of Action.
A consumer may bring a civil action for the violations of the FDPA to enjoin further violations and to recover actual damages. "Actual damages" means:

- the demonstrable economic value to the injured person of exclusive control of the personal data processed in violation of the FDPA, or the economic value to the controller or processor of the personal data processed in violation of the FDPA, whichever is greater; and
- the amount necessary to compensate the person for reputational harm and emotional distress resulting from the violation.

Thirty days prior to filing an action, a first party claimant must provide written notice of the basis for the action to the defendant and the Commission. If the defendant fails to resolve the basis for the action within the 30-day period, the claimant may bring the action without any further notice.

Annual Fee on Data Collectors.
Beginning on or after January 1, 2023, an annual fee is imposed upon every data controller or data processor that is required to register with the Commission. The Commission must share with the Department of Revenue a complete directory of all data controllers and processors registered with the Commission for the purposes of assessing the annual fee.

Consumer Privacy Account.
All receipts from the registration fees, imposition of administrative fines, civil penalties, and the annual data collectors fee must be deposited into the Consumer Privacy Account created in the State Treasury. Moneys in the account may only be used for the Commission and for the recovery of costs and attorneys' fees accrued by the Attorney General.

Preemption.
Local governments are preempted from adopting any laws, ordinances, or regulations regarding the processing of personal data by controllers or processors. Local laws, ordinances, or regulations adopted prior to July 1, 2021, are not superseded or preempted.

Appropriation: None.

Fiscal Note: Preliminary fiscal note available.

Effective Date: The bill takes effect on July 31, 2022.