Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

State Government, Elections & Information Technology Committee

HB 2278

Brief Description: Concerning personal information privacy protections in government entities.

Sponsors: Representatives Morris, Hudgins, Smith, Slatter, Tharinger, Macri, Young, Kloba and Appleton.

Brief Summary of Bill

- Requires each state agency to designate a privacy officer to reduce the use and retention of personal information by the agency.
- Requires each privacy officer to report to the Office of Privacy and Data Protection by December 15, 2018.
- Prohibits government entities from selling personal identification numbers and personal financial and health information.

Hearing Date: 1/16/18

Staff: Sean Flynn (786-7124).

Background:

Privacy and Personal Information. Personal information and privacy interests are protected under various provisions of state law. Personal privacy is protected from unreasonable state intrusion under Article 1, section 7 of the state Constitution. The Public Records Act (PRA), also protects a person's right to privacy under certain circumstances if disclosure would be highly offensive to the reasonable person, and is not of legitimate public concern. The PRA exempts personal information of public employees and officials maintained in public agency files from disclosure to the extent necessary to protect such person's right to privacy. Certain personal information related to investigative law enforcement records also is exempt from disclosure in order to protect a person's privacy.

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

The PRA also exempts certain personal information of public employee personnel records, including childcare enrollment, public employees and officials, tax assessments, personal financial information, driver's license records, vehicle license information associated with certain agencies conducting investigations, and 911 emergency systems contact information. Various other areas of state law protect privacy interests through confidentiality and other non-disclosure requirements.

Office of Privacy and Data Protection. In 2011 the Consolidated Technology Services (CTS) agency was created as part of a reorganization of state government information technology (IT) infrastructure functions and services. The CTS provides information services to public agencies, operates the state data center, and offers IT services, including data security and storage.

In 2016 the Office of Privacy and Data Protection (OPDP) was created within the CTS. The Chief Privacy Officer is appointed by the Chief Information Officer and serves as the director of the OPDP. The OPDP is the central point of contact for state agencies on policy matters involving data privacy and protection, and provides annual privacy training for state agencies, coordinates agency data protection, conducts an annual review, and reviews major state agency projects involving personally identifiable information.

Summary of Bill:

Each state agency must designate a privacy officer to work with the OPDP to develop agency policy that reduces the use and retention of personal information. Each privacy officer must complete a training course through the OPDP at least every four years.

By December 15, 2018, each privacy officer must create a work plan to report to the OPDP. The work plan must take inventory of all personal information prepared and retained by the agency, including the type of information, the purpose for its collection, and the extent to which such information is protected from unauthorized disclosure.

The plan also must include a map of the physical and digital location of the personal information collected by the agency. Personal information includes a person's name, social security number, state driver's license or identification card, financial account numbers, credit or debit card numbers, and security codes. The inventory and map created for the work plan is exempt from public disclosure under the PRA to the extent it reveals the location of personal information.

A government entity is prohibited from selling personal identification numbers issued by a government entity. A government entity also is prohibited from selling personal financial and health information, including information that is identifiable to an individual and commonly used for financial or health care purposes, including account information and access codes or passwords, as well as information gathered for account security purposes or for account access, or information that relates to medical history or status.

Appropriation: None.

Fiscal Note: Requested on January 15, 2017.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.