AMENDED IN SENATE MARCH 31, 2016

SENATE BILL No. 1444

Introduced by Senator Hertzberg

February 19, 2016

An act to ~~amend~~ *add* Section ~~1798.21 of~~ *1798.21.5 to* the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 1444, as amended, Hertzberg. ~~Personal information: privacy: state agencies: mitigation and response plans.~~ *State government: computerized personal information security plans.*

~~Existing law authorizes~~ *The Information Practices Act of 1977 requires* an agency, as defined, to maintain in its records only that personal ~~information~~ *information, as defined,* that is relevant and necessary to accomplish a purpose of the ~~agency,~~ *agency* required or authorized by the California Constitution or ~~statute,~~ *statute* or mandated by the federal government. ~~Existing~~ *That* law requires each ~~state~~ agency ~~that maintains personal information~~ to establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with *this* law, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to the security or integrity of the records that could result in any injury. Existing law requires an agency that owns or licenses computerized data that includes personal ~~information, as defined,~~ *information* to disclose a breach of the security of the system in the most expedient time possible and without unreasonable delay, as specified.

This bill would require ~~a state~~ *an* agency that owns or licenses computerized data that includes personal information to prepare ~~a mitigation and response plan for breach of the database that contains~~

~~the personal information.~~ *a computerized personal information security plan that details the agency's strategy to respond to a security breach of computerized personal information and associated consequences caused by the disclosed personal information. The bill would make legislative findings and declarations in this regard.*

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. The Legislature finds and declares all of the following:

(a) The Attorney General reported that since 2012, 657 data breaches of the kind affecting more than 500 Californians have exposed over 49 million records to fraudulent use.

(b) Malware and hacking attacks have risen dramatically in the past four years and account for a vast majority of the records that have been breached. These types of attacks present the greatest risk for massive disclosure of sensitive personal information, including, among others, social security numbers, driver's licenses, and dates of birth.

(c) Numerous state agencies hold records of millions of Californians and present the potential for large breaches of personal information in the future.

(d) Information technology professionals consider data breaches to be inevitable for organizations of all sizes and recommend the development and regular updating of plans and procedures designed to detect and halt breaches, notify affected Californians, and mitigate the damage caused by the data breaches.

SEC. 2. Section 1798.21.5 is added to the Civil Code, to read:

1798.21.5. An agency that owns or licenses computerized data that includes personal information shall prepare a computerized personal information security plan that details the agency's strategy to respond to a security breach of computerized personal information and associated consequences caused by the disclosed personal information. A computerized personal information security plan shall include, but is not limited to, all of the following:

(a) A statement of the purpose and objectives for the plan.

(b) An inventory of the computerized personal information stored or transmitted by the agency.

(c) Identification of resources necessary to implement the plan.

(d) Identification of an incident response team tasked with mitigating and responding to a breach, or an imminent threat of a breach, to the security of computerized personal information.

(e) Procedures for communications within the incident response team and between the incident response team, other individuals within the agency, and individuals outside the agency that need to be notified in the event of a breach of the security of computerized personal information.

(f) Policies for training the incident response team and the agency on the implementation of the computerized personal information security plan, including, but not limited to, the use of practice drills.

(g) A process to review and improve the computerized personal information security plan.

~~SECTION 1. Section 1798.21 of the Civil Code is amended to read:~~

~~1798.21. (a) Each agency shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of this chapter, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to the security or integrity of the records that could result in any injury.~~

~~(b) An agency that owns or licenses computerized data that includes personal information shall prepare a mitigation and response plan for breach of the database that contains the personal information.~~

O