AMENDED IN ASSEMBLY APRIL 27, 2015

AMENDED IN ASSEMBLY MARCH 26, 2015

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL No. 83

Introduced by Assembly Member Gatto

January 6, 2015

An act to amend Section 1798.81.5 of the Civil Code, relating to personal data.

LEGISLATIVE COUNSEL'S DIGEST

AB 83, as amended, Gatto. Information Practices Act of 1977.

Existing law requires a person or business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

This bill would define "reasonable security procedures and practices" for purposes of these provisions as requiring, at a minimum, ~~the encryption of private data to the degree that any reasonably prudent business would provide,~~ *security of personal information, including geophysical location information, to the degree that any reasonably prudent business would provide*, as specified. ~~The bill would define "private data" to include specified types personally identifying medical, financial, and geophysical information. The bill would also authorize the Department of Justice to specify security procedures, practices, and technical standards that it deems to be presumptively reasonable within a particular industry.~~

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

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

SECTION 1. Section 1798.81.5 of the Civil Code is amended to read:

1798.81.5. (a) (1) It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information.

(2) For the purpose of this section, the terms "own" and "license" include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term "maintain" includes personal information that a business maintains but does not own or license.

(b) A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(c) A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is not subject to subdivision (b) shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(d) For purposes of this section, the following terms have the following meanings:

(1) "Personal information" means an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Geophysical location information.

(2) "Geophysical location information" means any personally identifiable information describing or concerning the duration of a transportation service provided to an individual, the location and route of a transportation service provided to an individual, or, if applicable, the monetary exchange associated with a transportation service provided to an individual.

~~(2)~~

(3) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.

~~(3)~~

(4) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

~~(4) "Private data" means any of the following information:~~

~~(A) Medical information.~~

~~(B) Personally identifiable financial information, as that term is defined in subdivision (b) of Section 4052 of the Financial Code.~~

~~(C) Geophysical location information.~~

~~(D) The combination of an individual's first name or first initial and his or her last name, with any of the following:~~

~~(i) Mother's maiden name.~~

~~(ii) Social Security Number.~~

~~(iii) Date of birth.~~

(e) The provisions of this section do not apply to any of the following:

(1) A provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1).

(2) A financial institution as defined in Section 4052 of the Financial Code and subject to the California Financial Information Privacy Act (Division 1.2 (commencing with Section 4050) of the Financial Code).

(3) A covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996 (HIPAA).

(4) An entity that obtains information under an agreement pursuant to Article 3 (commencing with Section 1800) of Chapter 1 of Division 2 of the Vehicle Code and is subject to the confidentiality requirements of the Vehicle Code.

(5) A business that is regulated by state or federal law providing greater protection to personal information than that provided by this section in regard to the subjects addressed by this section. Compliance with that state or federal law shall be deemed compliance with this section with regard to those subjects. This paragraph does not relieve a business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information.

(f) For purposes of this section, "reasonable security procedures and practices" as they pertain to the storage and transmission of ~~private data~~ *personal information* shall require, at a minimum, the ~~encryption~~ *security* of that information to the degree that any reasonably prudent business would ~~provide, taking into account factors, including, but not limited to, the business' size, available technology, publically available threat information, generally accepted standards, and the customs and practices of the specific industry within which the business operates, to the extent commercially reasonable.~~ *provide. All of the following shall also apply:*

(1) At a minimum, the business shall:

(A) Identify reasonably foreseeable internal and external risks to the privacy and security of personal information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of the information.

(B) Establish, implement, and maintain safeguards reasonably designed to ensure the security of the personal information, including, but not limited to, protecting against unauthorized loss, misuse, alteration, destruction, access to, or use of the information.

(C) Regularly assess the sufficiency of any safeguards in place to control reasonably foreseeable internal and external risks, and evaluate and adjust those safeguards in light of the assessment.

(D) Evaluate and adjust any material changes in the operations or business arrangements of the business, or any other circumstances, that create a material impact on the privacy or security of personal information under control of the business.

(2) The reasonableness of the security procedures and practices shall be determined in light of all of the following:

(A) The degree of the privacy risk associated with the personal information under the business's control.

(B) The foreseeability of threats to the security of the information.

(C) The existence of widely accepted practices in administrative, technical, and physical safeguards for protecting personal information.

(D) The cost of implementing and regularly reviewing the safeguards.

~~(g) The Department of Justice may, at its discretion, specify security procedures and practices, including related technical standards, that it deems to be presumptively reasonable within a particular industry.~~

O