

AMENDED IN SENATE JULY 15, 2015

AMENDED IN SENATE JUNE 25, 2015

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.~~
Personal data.

Existing law requires a person or business that owns, licenses, or maintains personal information, *as defined*, 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”~~ *expand the definition of “personal information”* for purposes of these provisions ~~as requiring, at a minimum, security of personal information, including to include any unique government-issued identification number, an individual’s geophysical location information and location, health insurance, or biometric information, or an individual’s signature.~~ *The bill would also define “reasonable security procedures and*

practices” for purposes of these provisions as requiring, at a minimum, security of personal information to the degree that any reasonably prudent business would provide, as specified.

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

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

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

3 1798.81.5. (a) (1) It is the intent of the Legislature to ensure
 4 that personal information about California residents is protected.
 5 To that end, the purpose of this section is to encourage businesses
 6 that own, license, or maintain personal information about
 7 Californians to provide reasonable security for that information.

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

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

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

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

29 (1) “Personal information” means either of the following:
 30 (A) An individual’s first name or first initial and his or her last
 31 name in combination with any one or more of the following data

1 elements, when either the name or the data elements are not
2 encrypted or redacted:

3 (i) Social security number, tax identification number, passport
4 number, or any other unique government-issued identification
5 number.

6 (ii) Driver’s license number or California identification card
7 number.

8 (iii) Account number, credit or debit card number, in
9 combination with any required security code, access code, or
10 password that would permit access to an individual’s financial
11 account.

12 (iv) Medical information.

13 (v) *Health insurance information.*

14 ~~(v)~~

15 (vi) Geophysical location information.

16 ~~(vi)~~

17 (vii) Biometric information.

18 ~~(vii)~~

19 (viii) Signature.

20 (B) Username or email address in combination with a password
21 or security question and answer that would permit access to an
22 online account.

23 (2) “Geophysical location information” means any location data
24 generated to assess the past or current location of, or travel by, an
25 individual, including, but not limited to, geographic coordinates,
26 street address, or WiFi positioning system.

27 (3) “Biometric information” means data generated by automatic
28 measurements of an individual’s biological characteristics that are
29 used by the owner or licensee to authenticate an individual’s
30 identity, such as a fingerprint, voice print, eye retinas or irises, or
31 other unique biological characteristic.

32 (4) “Medical information” means any individually identifiable
33 information, in electronic or physical form, regarding the
34 individual’s medical history or medical treatment or diagnosis by
35 a health care professional.

36 (5) “Health insurance information” means an individual’s
37 insurance policy number or subscribed identification number, any
38 unique identifier used by a health insurer to identify the individual,
39 or any information in an individual’s application and claims history,
40 including any appeals records.

1 (6) “Personal information” does not include publicly available
2 information that is lawfully made available to the general public
3 from federal, state, or local government records.

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

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

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

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

18 (4) An entity that obtains information under an agreement
19 pursuant to Article 3 (commencing with Section 1800) of Chapter
20 1 of Division 2 of the Vehicle Code and is subject to the
21 confidentiality requirements of the Vehicle Code.

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

30 (f) For purposes of this section, “reasonable security procedures
31 and practices” as they pertain to the storage and transmission of
32 personal information shall require, at a minimum, the security of
33 that information to the degree that any reasonably prudent business
34 would provide. All of the following shall also apply:

35 (1) At a minimum, the business shall:

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

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

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

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

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

14 (A) The type of personal information under the business's
15 control.

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

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

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