

AMENDED IN SENATE AUGUST 19, 2016  
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. 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 expand the definition of “personal information” for purposes of these provisions to include ~~any unique~~ *an individual tax identification number, passport number, military identification, number government-issued employment identification number, an individual’s geophysical location, health insurance, geolocation information, or biometric information, or an individual’s signature.* *information.* The

bill would also define “reasonable security procedures and practices” for purposes of these provisions as ~~requiring, at a minimum,~~ *requiring* 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~~, *number, individual tax identification*  
4 *number, passport number, military identification number, or*  
5 *government issued employment identification 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 (vi) *Geolocation information.*

15 (vii) *Biometric information.*

16 (B) A username or email address in combination with a  
17 password or security question and answer that would permit access  
18 to an online account.

19 (2) *“Geolocation information” means location data generated*  
20 *by a consumer device capable of connecting to the Internet that*  
21 *directly identifies the precise physical location of the identified*  
22 *individual at particular times and that is compiled and retained.*  
23 *“Geolocation information” does not include the contents of a*  
24 *communication or information used solely for 911 emergency*  
25 *purposes.*

26 (3) *“Biometric information” means data generated by automatic*  
27 *measurements of an individual’s fingerprint, voice print, eye retinas*  
28 *or irises, identifying DNA information, or unique facial*  
29 *characteristics, which are used by the owner or licensee to uniquely*  
30 *authenticate an individual’s identity.*

31 ~~(2)~~

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 ~~(3)~~

37 (5) *“Health insurance information” means an individual’s health*  
38 *insurance policy number or subscriber identification number, any*  
39 *unique identifier used by a health insurer to identify the individual,*

1 or any *medical* information in an individual's *insurance* application  
2 and claims history, including any appeals records.

3 ~~(4)~~

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

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

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

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

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

21 (4) An entity that obtains information under an agreement  
22 pursuant to Article 3 (commencing with Section 1800) of Chapter  
23 1 of Division 2 of the Vehicle Code and is subject to the  
24 confidentiality requirements of the Vehicle Code.

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

33 (f) *For purposes of this section, "reasonable security procedures*  
34 *and practices" as they pertain to the storage and transmission of*  
35 *personal information shall require the security of that information*  
36 *to the degree that any reasonably prudent business would provide.*  
37 *All of the following shall also apply:*

38 (1) *The business shall undertake reasonable efforts, appropriate*  
39 *to the nature of the information, to do the following:*

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

5 (B) Establish, implement, and maintain safeguards reasonably  
6 designed to secure the personal information, including, but not  
7 limited to, protecting against unauthorized access, acquisition,  
8 destruction, use, modification, or disclosure of the information.

9 (C) Regularly assess the sufficiency of the safeguards required  
10 pursuant to subparagraph (B) to control reasonably foreseeable  
11 internal and external risks, and evaluate and adjust those  
12 safeguards in light of the assessment.

13 (2) The reasonableness of the security procedures and practices  
14 appropriate to the nature of the information shall be determined  
15 in light of all of the following:

16 (A) The type of personal information under the business's  
17 control.

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

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

23 (D) The cost of implementing and regularly assessing the  
24 safeguards.

25 (E) The size of the business.

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

28 1798.81.5. (a) (1) It is the intent of the Legislature to ensure  
29 that personal information about California residents is protected.  
30 To that end, the purpose of this section is to encourage businesses  
31 that own, license, or maintain personal information about  
32 Californians to provide reasonable security for that information.

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

39 (b) A business that owns, licenses, or maintains personal  
40 information about a California resident shall implement and

1 maintain reasonable security procedures and practices appropriate  
2 to the nature of the information, to protect the personal information  
3 from unauthorized access, destruction, use, modification, or  
4 disclosure.

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

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

14 (1) “Personal information” means either of the following:

15 (A) An individual’s first name or first initial and his or her last  
16 name in combination with any one or more of the following data  
17 elements, when either the name or the data elements are not  
18 encrypted or redacted:

19 (i) Social security number, tax identification number, passport  
20 number, or any other unique government-issued identification  
21 number.

22 (ii) Driver’s license number or California identification card  
23 number.

24 (iii) Account number, credit or debit card number, in  
25 combination with any required security code, access code, or  
26 password that would permit access to an individual’s financial  
27 account.

28 (iv) Medical information.

29 (v) Health insurance information.

30 (vi) Geophysical location information.

31 (vii) Biometric information.

32 (viii) Signature.

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

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

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

6     ~~(4) “Medical information” means any individually identifiable~~  
7 ~~information, in electronic or physical form, regarding the~~  
8 ~~individual’s medical history or medical treatment or diagnosis by~~  
9 ~~a health care professional.~~

10    ~~(5) “Health insurance information” means an individual’s~~  
11 ~~insurance policy number or subscribed identification number, any~~  
12 ~~unique identifier used by a health insurer to identify the individual,~~  
13 ~~or any information in an individual’s application and claims history,~~  
14 ~~including any appeals records.~~

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

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

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

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

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

32    ~~(4) An entity that obtains information under an agreement~~  
33 ~~pursuant to Article 3 (commencing with Section 1800) of Chapter~~  
34 ~~1 of Division 2 of the Vehicle Code and is subject to the~~  
35 ~~confidentiality requirements of the Vehicle Code.~~

36    ~~(5) A business that is regulated by state or federal law providing~~  
37 ~~greater protection to personal information than that provided by~~  
38 ~~this section in regard to the subjects addressed by this section.~~  
39 ~~Compliance with that state or federal law shall be deemed~~  
40 ~~compliance with this section with regard to those subjects. This~~

1 paragraph does not relieve a business from a duty to comply with  
2 any other requirements of other state and federal law regarding  
3 the protection and privacy of personal information.

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

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

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

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

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

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

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

27 (A) The type of personal information under the business’s  
28 control.

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

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

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