

## Cal Civ Code § 1798.29

Deering's California Codes are current through the 2024 Regular Session Ch 1

*Deering's California Codes Annotated > CIVIL CODE (§§ 1 — 7021) > Division 3 Obligations (Pts. 1 — 4) > Part 4 Obligations Arising from Particular Transactions (Titles 1 — 22) > Title 1.8 Personal Data (Ch. 1) > Chapter 1 Information Practices Act of 1977 (Arts. 1 — 12) > Article 7 Accounting of Disclosures (§§ 1798.25 — 1798.29)*

### **§ 1798.29. Disclosure of breach of security by agency that owns or maintains computerized data**

---

(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described in paragraph (2) under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

**(B)** The title and headings in the notice shall be clearly and conspicuously displayed.

**(C)** The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

**(D)** For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[name of institution / logo] date: [insert date]	
Notice of data breach	
What Happened?	
What Information Was Involved?	
What We Are Doing.	
What You Can Do.	
Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to [internet website]

**(E)** For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

**(2)** The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

**(A)** The name and contact information of the reporting agency subject to this section.

**(B)** A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

**(C)** If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

**(D)** Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

**(E)** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

**(F)** The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.

**(3)** At the discretion of the agency, the security breach notification may also include any of the following:

**(A)** Information about what the agency has done to protect individuals whose information has been breached.

**(B)** Advice on steps that people whose information has been breached may take to protect themselves.

**(e)** Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within Article 1 (commencing with Section 7923.600) of Chapter 1 of Part 5 of Division 10 of Title 1 of the Government Code.

**(f)** For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

**(g)** For purposes of this section, "personal information" means either of the following:

**(1)** An individual's first name or first initial and 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:

**(A)** Social security number.

**(B)** Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

**(C)** Account number or 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)** Health insurance information.

**(F)** Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

**(G)** Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

**(H)** Genetic data.

**(2)** A username or email address, in combination with a password or security question and answer that would permit access to an online account.

**(h)**

**(1)** For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

**(2)** For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

**(3)** For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

**(4)** For purposes of this section, "encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

**(5)** For purposes of this section, "genetic data" means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

**(i)** For purposes of this section, "notice" may be provided by one of the following methods:

**(1)** Written notice.

**(2)** Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

**(3)** Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

**(A)** Email notice when the agency has an email address for the subject persons.

**(B)** Conspicuous posting, for a minimum of 30 days, of the notice on the agency's internet website, if the agency maintains one. For purposes of this subparagraph, conspicuous posting on the agency's internet website means providing a link to the notice on the home page or first significant page after entering the internet website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

**(C)** Notification to major statewide media and the Office of Information Security within the Department of Technology.

**(4)** In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same username or email address and password or security question or answer.

**(5)** In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

**(j)** Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

**(k)** Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, "agency" includes a local agency, as defined in Section 7920.510 of the Government Code.

**(l)** For purposes of this section, "encryption key" and "security credential" mean the confidential key or process designed to render the data usable, readable, and decipherable.

**(m)** Notwithstanding any other law, the State Bar of California shall comply with this section. This subdivision shall not be construed to apply other provisions of this chapter to the State Bar.

## History

---

Added Stats 2002 ch 1054 § 2 (AB 700), operative July 1, 2003. Amended Stats 2007 ch 699 § 4 (AB 1298), effective January 1, 2008; Stats 2011 ch 197 § 1 (SB 24), effective January 1, 2012; Stats 2013 ch 395 § 1 (AB 1149) effective January 1, 2014, ch 396 § 1.5 (SB 46), effective January 1, 2014; Stats 2015 ch 522 § 1 (AB 964), effective January 1, 2016, ch 532 § 1 (SB 34), effective January 1, 2016, ch 543 § 1.3 (SB 570), effective January 1, 2016; Stats 2016 ch 86 § 20 (SB 1171), effective January 1, 2017, Stats 2016 ch 337 § 1 (AB 2828), effective January 1, 2017 (ch 337 prevails); Stats 2019 ch 750 § 1 (AB 1130), effective January 1, 2020; Stats 2021 ch 527 § 1 (AB 825), effective January 1, 2022; Stats 2021 ch 615 § 45 (AB 474), effective January 1, 2022 (ch 527 prevails); Stats 2022 ch 28 § 22 (SB 1380), effective January 1, 2023; Stats 2022 ch 419 § 14 (AB 2958), effective September 18, 2022 (ch 419 prevails).

Deering's California Codes Annotated  
Copyright © 2024 All rights reserved.

---

End of Document