FREQUENTLY ASKED QUESTIONS ABOUT THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 (CCPA)

Date: 31 July 2018

U.S. Data Protection, Privacy, and Security Alert

Following are answers to common questions our clients have asked since CCPA was enacted. Please check back for new and updated FAQs in the coming months.

FAQ 1: WHY DID THE CALIFORNIA LEGISLATURE ENACT CCPA?

CCPA was first introduced in the California legislature in February 2017. The early version of CCPA focused on cable and Internet service companies because "Congress and the Trump administration effectively halted a set of federal consumer privacy protection rules on Internet service providers that were scheduled to take effect."[1] After a series of committee reviews and amendments in April, June and September, the emphasis on cable and internet service companies lessened and CCPA was moved to the inactive file on September 16, 2017.

Approximately one month later a ballot initiative[2] titled "The California Consumer Right to Privacy Act of 2018" ("Ballot Initiative")[3] was filed with the California Attorney General on October 12, 2017. The stated purpose of the Ballot Initiative was to "give [Californians] important new consumer privacy rights to take back control of [their] personal information."[4]

By May 3, 2018, proponents of the Ballot Initiative announced that they had sufficient signatures to add the Ballot Initiative to California's November 2018 statewide general election.[5] The Ballot Initiative was opposed, however, by a coalition of businesses called "Committee to Protect California Jobs,"[6] which characterized the Ballot Initiative as "limiting [our] choices, hurting [our] businesses, and cutting [our] connection to the global economy."[7] Meanwhile, after eight months as an inactive file, CCPA was resurrected on June 21, 2018 and amended so that, by its terms, it only would take effect if the Ballot Initiative were withdrawn.[8] The Ballot Initiative's proponents agreed to withdraw the Ballot Initiative, and a week after its resurrection, CCPA became law on June 28, 2018.

CCPA is consistent with California's history of actively protecting its residents' privacy rights. In 2004, the California Online Privacy Protection Act ("CalOPPA")[9] went into effect as the first US state law requiring website operators to post privacy policies describing their information handling practices.[10] Like CalOPPA, CCPA is focused on protecting California residents by requiring notice about a business's personal information handling practices. CCPA regulates an entity "that does business" in California and meets specified thresholds (albeit low ones, as described below). CalOPPA is not limited to California businesses — CalOPPA applies to any operator of a "Web site located on the Internet or an online service" that collects and maintains personal information from a California resident who uses or visits the Web site or online service.[11] CCPA's scope is significantly broader:

©2005-2026 K&L Gates LLP. All Rights Reserved.

CCPA has a more expansive definition of personal information than CalOPPA and applies to “collection and sale of all personal information” by a covered business, not just personal information collected online.[12]

FAQ 2: WHO RECEIVES NEW RIGHTS UNDER CCPA? WHAT IS A “CONSUMER”?

CCPA's new rights are for “consumers.”[13] Under CCPA, a consumer is a California “resident” as defined in California's personal income tax regulations, i.e., any natural person “enjoying the benefit and protection of [California] laws and government” who is in California “for other than a temporary or transitory purpose” or “domiciled” in California but “outside the State for a temporary or transitory purpose.” [14]

FAQ 3: WHAT IS THE DEFINITION OF “PERSONAL INFORMATION” TO WHICH CCPA APPLIES?

CCPA defines “personal information” as information that “identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”[15] This definition is broader than the Federal Trade Commission's definition of personal information[16] and similar in scope to the definition of personal data under GDPR.[17]

To illustrate, but not limit, its broad definition of personal information, CCPA enumerates eleven specific categories: (i) identifiers, such as a “unique personal identifier” (a defined term)[18] and “online identifier Internet Protocol address”; (ii) “characteristics of protected classifications under California or federal law”; (iii) “commercial information,” such as including records of products or services purchased and other purchasing or consuming histories or tendencies; (iv) biometric information, a defined term that means physiological, biological and behavioral characteristics and includes the traditional fingerprint and retinal scan but also keystroke and gait patterns as well as “sleep, health and exercise data that contain identifying information”; (v) “Internet or other electronic network activity information,” such as browsing history or “interaction … with an advertisement”; (vi) geolocation data; (vii) audio, electronic, visual, thermal, olfactory or similar information; (viii) professional or employment-related information; (ix) education information that is not public as defined in the federal Family Educational Rights and Privacy Act[19], and (x) inferences, which is a defined term meaning the “derivation of information … assumptions, or conclusions from … another source of information,” derived from data drawn from any of the information identified above to create a profile about a consumer's “preferences, characteristics, psychological trends, preferences [sic], predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.”

FAQ 4: WHAT INFORMATION IS EXCLUDED FROM CCPA'S DEFINITION OF PERSONAL INFORMATION?

CCPA's definition of personal information excludes “publicly available information,” which means information “lawfully made available from federal, state, or local government records, if any conditions associated with such information” but excludes biometric information collected without the consumer's knowledge and personal

©2005-2026 K&L Gates LLP. All Rights Reserved.

information used for a purpose different from the one for which the data is maintained and made available in the government records or otherwise publicly maintained.[20]

Personal information also does not include “de-identified” consumer information, which cannot “reasonably identify … or be linked to” a particular person,[21] or “aggregate” consumer information, which is “not linked or reasonably linkable to any consumer or household, including via a device”[22]. Also excepted from CCPA is personal information:

- collected, used, sold or disclosed pursuant to the Gramm-Leach-Blilely Act[23] or the Driver's Privacy Protection Act of 1995[24], but only if CCPA “is in conflict” with those laws; and
- sold to or from a consumer reporting agency (as defined in the Fair Credit Reporting Act)[25] when the personal information is “reported in, or used to generate,”[26] a consumer credit report.[27]

FAQ 5: WHAT BUSINESSES MUST COMPLY WITH CCPA? DOES CCPA APPLY TO NON-PROFITS?

CCPA applies to a for-profit entity that:

- collects consumers' personal information directly or through a third party; and
- alone or jointly determines the purposes and means of the processing[28] of consumers' personal information; and
- does business in the State of California; and
- meets one of the following thresholds:
  - has annual gross revenues in excess of $25,000,000;
  - alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; and
  - derives 50 percent or more of its annual revenues from selling consumers' personal information.[29]

California is the world's fifth largest economy,[30] and as a result CCPA covers a large number of businesses inside and outside California. It is unclear at this point whether the $25,000,000 threshold encompasses *worldwide* or only California annual gross revenue. And, as drafted, the economic thresholds will sweep in many small businesses that do not meet the $25,000,000 gross revenue threshold. Any entity that controls or is controlled by a business and shares common branding with a business that meets the above criteria also is subject to CCPA.

A non-profit entity is not subject to CCPA because it does not operate “for the profit or financial benefit”[31] of its owners.

A “covered entity”[32] subject to the Health Insurance Portability and Accountability Act of 1996[33] is not subject to CCPA with respect to the protected health information (“PHI”)[34] that it collects from a consumer but could be subject to CCPA for any personal information (as defined in CCPA) collected that is not PHI.

©2005-2026 K&L Gates LLP. All Rights Reserved.

FAQ 6: WHAT NEW RIGHTS DO CONSUMERS RECEIVE UNDER CCPA?

#1 – Right to Know

The right to know has two main components.

The first right-to-know component relates to personal information that is *collected* or *sold* or *disclosed* about a specific consumer.

> When a business *collects* personal information from or about a consumer, the consumer can submit a request (subject to verification of the consumer's identity)[35] for:
>
> - the categories of personal information that the business has collected about him or her in the 12 months preceding the request[36] and "specific pieces" of that personal information;[37]
> - the source from which the personal information was collected;[38]
> - the business purpose or commercial purpose (each of which are defined terms[39]) for collecting or selling the personal information;[40] and
> - the categories of third parties with whom or which the personal information is shared.[41]
>
> When a business *sells or discloses for a business purpose*[42] personal information about a consumer, the business also must disclose to the consumer the categories of personal information sold or disclosed for a business purpose about him or her and the parties to whom or which each category of personal information was sold.[43]

The second right-to-know component requires a business to make "reasonably accessible"[44] general disclosures. Specifically, a covered business must disclose, through its website privacy policy or elsewhere on its website:

- *at or before collection of personal information*, the categories of personal information collected and how the business will use the information;[45]
- how a consumer can exercise his or her right to know about the collection and sale or other disclosure of his or her personal information;[46]
- the categories of personal information collected during the preceding 12 months;[47] and
- separate lists of the categories of personal information sold and disclosed during the preceding 12 months *or* a statement that no sale or disclosure was made.[48]

Neither right-to-know requirement mandates a business to retain information collected for a single transaction or to link de-identified information to personal information unless, in either case, the business' usual practice is to do so.[49]

#2 – Right to Access

©2005-2026 K&L Gates LLP. All Rights Reserved.

A consumer can request a copy of the specific personal information that a business retains about him or her. Upon receipt of a verifiable consumer request for access, the business must provide the "specific pieces of personal information" that it retains about the consumer. The business must provide the personal information free of charge either through the consumer's "account"[50] with the business or, at the consumer's option, by mail or in a readily usable electronic format "that allows the consumer to transmit the information to another entity without hindrance."[51] The business is obligated to respond to no more than two right-to-access requests in a 12-month period.[52] The right to access does not apply to information collected for a single transaction as long as the information is not sold or retained for the purpose of linking it to personal information.[53]

As with the right to know, a business is not required to retain information collected for a single transaction or to link de-identified information to personal information unless, in either case, the business' usual practice is to do so.[54]

#3 – Right to Deletion

A consumer may submit and a business must honor a verifiable consumer request for deletion of any personal information that the business has collected from the consumer.[55] The business also must ensure that its service providers[56] delete the consumer's personal information.

The deletion right does not apply when the business needs the personal information:

- to complete the transaction or provide a good or service requested by the consumer for which the business collected the personal information or otherwise perform a contract between the business and the consumer;
- to detect or prevent security incidents or illegal activity;
- to identify and correct errors that impair existing functionality;
- for the exercise of a legal right or to ensure another consumer can exercise his or her legal right;
- to comply with the California Electronic Communications Privacy Act;[57]
- to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest[58] if deletion of the personal information is likely to make the research impossible or seriously impair it;
- solely for internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;
- to comply with a legal obligation; or
- for lawful internal uses that are compatible with the context in which the consumer provided the personal information to the business.

Although certain of these exceptions are broad, the business still must take care that they are part of the business' privacy policy or other website disclosures consistent with the right to know.[59]

#4a – Right to Opt Out

©2005-2026 K&L Gates LLP. All Rights Reserved.

A consumer may use a right to opt out to instruct a business that sells personal information not to sell the consumer's personal information. Once a consumer opts out, the business must honor the opt-out request for at least 12 months, but subsequently may sell the consumer's personal information if the consumer provides his or her “express authorization”.[60]

Absent opting out, the business can sell the consumer's personal information as long as the business has complied with the relevant disclosure requirements. That is, a business that sells personal information must:

- add a conspicuous “Do Not Sell My Personal Information” link on the homepage[61] of its website to a separate web page that enables the consumer to opt out (“Opt-out Page”) (note that a business can avoid the “Do Not Sell My Personal Information” home page link by maintaining a separate and conspicuous California-consumer-specific webpage that includes the required disclosure);[62]
- disclose in its privacy policy or any “California-specific description of consumers' privacy rights”[63] the right to opt out, together with a link to the Opt-out Page; and
- train “all individuals responsible for handling consumer inquiries” about the opt-out right and how a consumer can exercise the right to opt out.

The right to opt out applies to consumers age 16 and older.

#4b – Right to Opt In for Consumers Under Age 16

Instead of an opt-out right, minors under age 16 have an opt-in right.[64] That is, CCPA prohibits the sale of personal information collected from a consumer who is:

- age 13 up to 16 *unless* the consumer has opted in; or
- under age 13 *unless* a parent or legal guardian has “affirmatively authorized”[65] the sale.

The prohibition of sale applies only if the business has “actual knowledge” of the minor's age.[66] A CCPA-covered business is deemed to have actual knowledge that it has collected personal information from children under age 16 if it “willfully disregards the consumer's age.”[67]

CCPA coordinates—at least in part—with the federal Children's Online Privacy Protection Act (“COPPA”).[68] COPPA requires operators of child-directed websites, mobile applications and other Internet-connected services[69] that are “directed to children”[70] to post a privacy policy and obtain verifiable parental consent before collecting personal information from children under age 13. Unlike COPPA, CCPA is not limited to Internet-connected services.

Like CCPA, COPPA has an actual knowledge qualifier. COPPA applies to an Internet-connected service for a general audience, i.e., not directed to children, only if its operator has “actual knowledge”[71] that children are providing personal information on or through the Internet-connected service. In practice, many operators of general-audience online services state in their privacy policies that the service is not directed to children under age 13 and that children under age 13 are not permitted to use it — and purposefully do not ask about users' ages to avoid actual knowledge.

#5 – Right to Equal Service and Price

©2005-2026 K&L Gates LLP. All Rights Reserved.

The right to equal service is intended to prevent a business from discriminating against a consumer who uses the rights granted by CCPA.[72] For example, a business cannot deny goods or services to a consumer, charge a consumer a different price, provide different or lower-quality goods or services to a consumer, or suggest a consumer will experience any of the foregoing simply because the consumer exercised his or her CCPA right to opt out.[73]

CCPA does, however, permit a business to offer different products or services if the difference is "reasonably related" to the value of the consumer's data. A business also may offer financial incentives to a consumer – including better quality or service levels or more favorable pricing ─ in exchange for the collection, sale or deletion (or absence of deletion) of his or her personal information if the better quality, service or pricing is "directly related" to the value of the consumer's data.[74] The consumer must, however, opt into ─ and have the right to opt out of ─ the "financial incentive program" after notice of the program's material terms.[75]

The California Attorney General's regulations "necessary to further the purposes" of CCPA[76] are expected to explain how to determine the value of consumer data and the difference between "reasonably related" value for price and quality differences and "directly related" value for financial incentives. In the meantime, as part of preparing for CCPA, businesses may wish to explore charging fees for products or services that were previously offered for free in order to offset the direct and indirect costs of CCPA compliance.

FAQ 7: HOW IS A SALE OF PERSONAL INFORMATION DIFFERENT FROM A DISCLOSURE FOR A "BUSINESS PURPOSE"?

CCPA defines "sell" broadly to include any communication or transfer of consumer's personal information by a CCPA-covered business to a third party "for monetary or other valuable consideration."[77] Disclosing personal information for a "business purpose" is different because the disclosure is for one of the enumerated "operational" purposes (described below) of the CCPA-covered business or its service provider.

A business generally may sell personal information orally, in writing, electronically or by "other means."[78] CCPA excludes the following from its definition of a sale:

when a consumer uses or directs ─ through "one or more deliberate interactions"[79] ─ the business to intentionally disclose personal information to a third party, as long as the third party does not subsequently sell the personal information (unless the sale is otherwise permitted under CCPA);

when a business uses or shares an identifier to inform others that the consumer has exercised the right to opt out[80];

when a business uses or shares personal information with a service provider "necessary to perform a business purposes *[sic]*", if:

- the business already provided CCPA-compliant notice about the use or sharing; *and*
- the service provider does not use the transferred personal information except as necessary to perform the business purpose[81]; or

©2005-2026 K&L Gates LLP. All Rights Reserved.

when a transfer of personal information that is part of a merger, acquisition, bankruptcy, or other transaction in which a third party assumes control of the business (in whole or part), if the transferee continues to honor the right to know and right to access, including notifying consumers in advance if the transferee will use or share the personal information in a new or different way.[82]

"Business purposes" are:

- "auditing" the interaction with the consumer and concurrent transactions, including counting ad impressions, verifying quality of ad impressions and "auditing compliance with this specification and other standards";
- detecting or preventing security incidents;
- debugging;
- short-term, transient use if the personal information is not disclosed and not used to build a profile or "otherwise alter an individual consumer's experience outside the current interaction," such as for "contextual customization of ads shown as part of the same interaction" (i.e., interest-based advertising);
- performing services on behalf of a CCPA-covered business or its service provider, such as customer service, order fulfillment, payment processing, financing and advertising, marketing or analytic services;
- undertaking internal research for "technological development and demonstration"; and
- verifying or maintaining quality or safety or improving or upgrading a service or device[83] owned, manufactured or controlled by or for the business.[84]

Any use of personal information for a business purpose must be reasonably necessary for, and proportionate to, the purpose for which the personal information is first processed or another contextually "compatible" operational purpose.[85]

FAQ 8: WHAT IS A "VERIFIABLE CONSUMER REQUEST" AND HOW DOES A BUSINESS RESPOND TO ONE?

CCPA defines a "verifiable consumer request" ("VCR") as a request made by or on behalf of a consumer to exercise his or her CCPA rights for which a business can reasonably verify the identity of the consumer or the consumer's representative.[86]

For the right to know and right to opt out, a CCPA-covered business must offer at least two methods for VCR submission.[87] One of these two methods must be a toll-free number and the other a website address (if the business has a website).[88] A business is required to respond to only two (2) requests from the same consumer over a 12-month period.[89] The VCR process must be free of charge to the consumer.

For any VCR, the business must respond in writing either through the consumer's account with the business if the consumer maintains an account with the business or, if the consumer does not maintain an account with the business, the consumer's choice of mail or electronic communication.[90] Once a consumer has submitted the VCR, the business has 45 days to respond and, as long as the business notifies the consumer within the first 45

©2005-2026 K&L Gates LLP. All Rights Reserved.

days that additional time is needed, up to 45 more days (or a total of 90 days). The response to the VCR must cover the 12-month period preceding the date on which the business received the VCR.[91]

By June 28, 2019, the California Attorney General is required to adopt regulations to help businesses determine when a request is a VCR.[92] CCPA deems a consumer's request "submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account" as a VCR.[93] But, a business may not require a consumer to create an account in order to submit a VCR.[94]

FAQ 9: HOW DOES CCPA APPLY TO A SERVICE PROVIDER THAT PROCESSES PERSONAL INFORMATION FOR A CCPA-COVERED BUSINESS?

A "service provider" is a for-profit entity that processes information on behalf of a CCPA-covered business.[95] CCPA requires that the business (i) enter into a written contract with the service provider prohibiting the service provider from undertaking any processing of the personal information other than for the specific purpose of performing the services specified in the written contract[96] and (ii) obtain "certification" that the service provider understands these restrictions.[97] When requested, the service provider must delete personal information it processes for the CCPA-covered business, subject to the same exceptions to the right to delete as the covered business.

The service provider is liable for its own violations of CCPA, and the business that discloses the personal information to the service provider also will be liable for the service provider's CCPA violations if the business had "actual knowledge or reason to believe" that the service provider intended to violate CCPA.[98]

FAQ 10: DOES CCPA HAVE EXCEPTIONS?

CCPA does not apply to a business that processes personal information when the personal information is used to:

- comply with federal, state, or local laws or a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons;
- cooperate with law enforcement agencies;
- exercise or defend legal claims;
- process "de-identified"[99] information or "aggregate consumer information";[100] or
- collect or sell personal information when "every aspect of that commercial conduct takes place wholly outside of California" ─ that is, CCPA does not apply if all personal information was collected while the person to whom the personal information relates was outside of California and no part of the sale of the personal information occurred in California.[101]

CCPA also does not apply if compliance would violate evidentiary privileges given under California law.[102]

FAQ 11: WHAT ARE THE PENALTIES FOR VIOLATING CCPA? DOES CCPA HAVE A PRIVATE RIGHT OF ACTION?

©2005-2026 K&L Gates LLP. All Rights Reserved.

The California Attorney General enforces CCPA, except that CCPA offers only a private right of action for "unauthorized access and exfiltration, theft, or disclosure" (i.e., a data breach).[103]

Attorney General Action

Prior to initiating an action for a CCPA violation, the California Attorney General must give the offending business, service provider or other person not less than 30 days to cure the alleged violation.[104] Thereafter:

- a business, service provider, or other person that *negligently* violates CCPA is subject to a civil penalty not to exceed $2,500 for each violation;[105] and
- a business, service provider or other person that *intentionally* violates CCPA is liable for a civil penalty of up to $7,500 per violation.[106]

Private Right of Action

A business may face a privacy right of action if it fails to implement and maintain reasonable security procedures and practices appropriate to the sensitivity of personal information processed by the business that causes a data breach.[107] Specifically, the consumer may recover the greater of statutory damages of $100 to $750 "per consumer per incident" and actual damages. In determining statutory damages, a court must evaluate the nature, seriousness and persistence of the violations, the number of violations, the length of time over which the violations occurred, the willfulness of the violations, and the business' "assets, liabilities and net worth."[108]

Before filing a lawsuit against the business for unreasonable security procedures, however, the consumer must provide 30 days' advance notice to the business of the allegedly violations:

- If the business cures the alleged violation and provides the consumer "an express written statement that the violations have been cured and that no further violations shall occur,"[109] the consumer cannot proceed with the lawsuit.
- If the business continues with its alleged violations, the consumer can file a lawsuit for the original, and any new, CCPA violation, including breaching the written statement.[110]

No notice is required if the consumer suffered actual pecuniary damages as a result of the business' failure to implement and maintain reasonable security procedures.[111]

The consumer also must notify the California Attorney General within 30 days after filing the lawsuit.[112] The Attorney General then has 30 days to decide whether to prosecute the violation, to allow the consumer to proceed with his or her private action, or to notify the consumer that "the consumer shall not proceed with the action." [113]

FAQ 12: WHAT ARE THE KEY SIMILARITIES BETWEEN CCPA AND GDPR?

1. CCPA and GDPR both view the privacy of personal information as a fundamental right.[114]

2. Both laws broadly define what is "personal," although CCPA's definition of personal information includes a reasonableness qualifier.

©2005-2026 K&L Gates LLP. All Rights Reserved.

CCPA	GDPR
Information that identifies, relates to, describes, is capable of being associated with, or could *reasonably* be linked, directly or indirectly, with a particular consumer or household.[115]	Information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier. [116]
Personal information categories include: ▪ "unique personal identifiers" (as defined);[117] ▪ geolocation data; ▪ purchasing, browsing and search histories; ▪ biometric information;[118] Notably, CCPA's personal information includes "olfactory" and "thermal" information linked to a consumer or household; and ▪ "purchasing or consumer tendencies"; all of which are quite broad and indefinite.	Identifiers include "name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[119]

Both laws have similarly defined the term for doing something with personal information — "processing" — as any operation performed on personal data, whether automated or otherwise.[120]

3. Like GDPR, CCPA offers individuals some rights to control how their personal information is used and disclosed.

CCPA	GDPR
Consumer rights include the right to: ▪ know what personal information is collected and whether it is disclosed; ▪ request access to personal information; ▪ request deletion of personal information collected from the consumer; ▪ opt out of the sale of the consumer's personal information; and ▪ receive collected personal information that a	Data subject rights include the right to: ▪ receive information about personal data processing, including categories of personal data, purpose of processing the personal data, recipients of the personal data and whether personal data is transferred across international borders; ▪ request access to personal data and have inaccurate personal data corrected; ▪ request the erasure of personal data;

©2005-2026 K&L Gates LLP. All Rights Reserved.

business has free of charge by mail or in a readily usable electronic format that allows the consumer to transmit the information to another entity.	▪ object to or restrict the processing of personal data; and ▪ request that personal data be transferred to another data controller or provided in a format that will permit such a transfer.[121]

4. Both CCPA and GDPR recognize the need for businesses to conduct due diligence on the third parties that assist them with personal information processing and to have the arrangements memorialized in a contract.[122]

5. Both CCPA and GDPR have potentially large regulatory fines:

CCPA	GDPR
▪ *Negligent* violations, up to $2,500 per violation. [123] ▪ *Intentional* violations, up to $7,500 per violation. [124]	Fines include: ▪ €10m or up to 2% of world annual turnover, whichever is greater, for, among others, violations of the general obligations of the controller or processor to process personal data securely or to perform diligence on processors and for personal data breach notifications;[125] ▪ up to 20,000,000 EUR or up to 4% of total worldwide annual turnover of the previous year, whichever is greater, for violations of data protection principles, consent, data subjects rights and cross-border data transfer requirements.[126]

Notes:

[1] *See* AB375 dated February 9, 2017, https://leginfo.legislature.ca.gov/faces/billVersionsCompareClient.xhtml?bill_id=201720180AB375&cversion=20170AB37599INT.

[2] California law permits eligible California voters to bypass the legislative process by submitting the text of a new law to the California Attorney General. If the "proponents" of the new law obtain the required minimum number of signatures, the proposed law is added to the ballot for the next general election. CAL. ELEC. CODE § 9000 et seq.

[3] The Ballot Initiative was organized by Californians for Consumer Privacy and is available at https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf.

[4] The California Attorney General summarized the Ballot Initiative as: "Gives consumers right to learn categories of personal information that businesses collect, sell, or disclose about them, and to whom information is sold or

©2005-2026 K&L Gates LLP. All Rights Reserved.

disclosed. Gives consumers right to prevent businesses from selling or disclosing their personal information. Prohibits businesses from discriminating against consumers who exercise these rights. Allows consumers to sue businesses for security breaches of consumers' data, even if consumers cannot prove injury. Allows for enforcement by consumers, whistleblowers, or public agencies. Imposes civil penalties. Applies to online and brick-and-mortar businesses that meet specific criteria." *See* https://oag.ca.gov/system/files/initiatives/pdfs/Title%20and%20Summary%20%2817-0039%29_0.pdf.

[5] The Ballot Initiative needed 365,880 signatures and 629,000 were obtained.

[6] Sponsored by the California Chamber of Commerce and a Coalition of Innovation Companies, Committee Major Funding from AT&T, Google and Facebook.

[7] *See* "Statement By The Committee To Protect California Jobs On Submission Of Signatures For Internet Regulation Ballot Measure," (May 3, 2018), https://californianewswire.com/statement-by-the-committee-to-protect-california-jobs-on-qualification-of-signatures-for-internet-regulation-ballot-measure/.

[8] CAL. CIV. CODE § 1798.198(b).

[9] CAL. BUS. & PROF. CODE §§ 22575–22579. Notably, CalOPPA is part of California's Business Code because CalOPPA regulates businesses that operate websites that collect personal information, whereas CCPA is part of its Civil Code, which reflects CCPA's emphasis on consumer rights.

[10] California has several other laws, including California Civil Code § 1798.83 (known as the "Shine the Light" law), which requires a business collecting personal information from its California customers and disclosing it to "third parties" for direct marketing purposes to take certain steps to inform customers of this practice and Privacy Rights for California Minors in the Digital World (CAL. BUS. & PROF. CODE §§ 22580–22582), which requires websites that are directed to or known to be used by California minors to offer a process for California minors to remove (or have removed) their own posted content and information.

[11] CAL. BUS. & PROF. CODE § 22577(c).

[12] CAL. BUS. & PROF. CODE § 22577(a).

[13] CAL. CIV. CODE § 1798.140(g).

[14] 18 CA ADC § 17014.

[15] CAL. CIV. CODE § 1798.140(o).

[16] "…information reasonably linked to a specific consumer, computer or other device." *See* Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[17] GDPR Article 1(1) defines personal data as any information "relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier."

[18] Unique identifier means a persistent identifier that can be used to recognize a consumer, a family, or a device (another defined term (CAL. CIV. CODE § 1798.140(j))) that is linked to a consumer or family, over time, and across different services, including, but not limited to, a device identifier; an Internet protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers; or other forms of persistent or probabilistic identifiers (yet another defined term (§ 1798.140(p))) that can be used to identify a particular consumer or device.

[19] 20 U.S.C. § 1232g.

[20] CAL. CIV. CODE § 1798.140(o)(2).

©2005-2026 K&L Gates LLP. All Rights Reserved.

[21] CAL. CIV. CODE § 1798.140(h).
[22] CAL. CIV. CODE § 1798.140(a).
[23] 15 U.S.C. §§ 6801–6809. Among other requirements, the Gramm-Leach-Blilely Act requires financial institutions (i.e., banks and securities firms as well as real estate appraisers; check printing, money wiring, check cashing, tax preparation, and credit counseling businesses; insurance underwriters and mortgage brokers (16 C.F.R. §313.3(k)) to provide notice about the procedures and policies implemented for protecting the privacy of non-public personal information, which is personally identifiable financial information that a financial institution obtains from or about an individual in connection with a financial product or service that is not publicly available.
[24] 18 U.S.C. §2721 et seq. The Driver's Privacy Protection Act prohibits the disclosure of drivers' personal information in a motor vehicle record by state departments of motor vehicles except for the uses listed in such Act.
[25]15 U.S.C. § 1681 et seq. The Fair Credit Reporting Act enacted procedures to ensure “accuracy and fairness of credit reporting” and thereby ensure “a respect for [a] consumer's right to privacy.” 15 U.S.C. § 1681(a).
[26] CAL. CIV. CODE § 1798.145(d).
[27] 15 U.S.C. § 1681a(d).
[28] “Processing” under CCPA means any operation or set of operations performed on personal information. CAL. CIV. CODE § 1798.140(q).
[29] CAL. CIV. CODE § 1798.140(c).
[30] Thomas Fuller, The Pleasure and Pain of Being California, the World's 5th-Largest Economy, N.Y. TIMES (May 7, 2018), https://www.nytimes.com/2018/05/07/us/california-economy-growth.html.
[31] CAL. CIV. CODE § 1798.140(c)(1).
[32] Covered entities are health plans, most health care providers and health care clearinghouses and their “business associates” (i.e., the third parties that support covered entities).
[33] HIPAA, Pub. L. 104–191.
[34] PHI is individually identifiable health information created or received by a covered entity.
[35] Also referred to as a “verifiable consumer request” which is defined in CAL. CIV. CODE § 1798.140(y) and subject to “regulations adopted by the Attorney General.” *See* FAQ 9.
[36] CAL. CIV. CODE §§ 1798.110, 130(a)(3)(B).
[37] CAL. CIV. CODE § 1798.100(a)(1), 110(a)(5).
[38] CAL. CIV. CODE § 1798.100(a)(2).
[39] Business purpose” is defined in 1798.140(d) as operational purposes reasonable and necessary for the purposes for which the personal information was collected. A “commercial purpose” as defined in 1798.140(f) is to advance the business' “commercial or economic interests” by “inducing” directly or indirectly a “commercial transaction” but excluding “noncommercial speech” such as “political speech and journalism.” *See* also FAQ 8.
[40] CAL. CIV. CODE § 1798.100(a)(3).
[41] CAL. CIV. CODE § 1798.100(a)(4).
[42] *See* FAQ 8: WHAT IS A “VERIFIABLE CONSUMER REQUEST” AND HOW DOES A BUSINESS RESPOND TO ONE?.
[43] CAL. CIV. CODE § 1798.115.
[44] CAL. CIV. CODE § 1798.130(a)(5).
[45] CAL. CIV. CODE § 1798.100(c).
[46] CAL. CIV. CODE § 1798.130(a)(5)(A).

©2005-2026 K&L Gates LLP. All Rights Reserved.

[47] CAL. CIV. CODE § 1798.130(a)(5)(B).
[48] CAL. CIV. CODE § 1798.130(a)(5)(C).
[49] CAL. CIV. CODE §§ 1798.100(e), 110(d).
[50] CAL. CIV. CODE § 1798.130(a)(2).
[51] CAL. CIV. CODE § 1798.100(d).
[52] CAL. CIV. CODE § 1798.100(d).
[53] CAL. CIV. CODE § 1798.100(e).
[54] CAL. CIV. CODE §§ 1798.100(e), 110(d).
[55] CAL. CIV. CODE § 1798.105.
[56] CAL. CIV. CODE § 1798.140(v). A “service provider” has a written contract with the business receiving the request and receives and processes (defined in CAL. CIV. CODE § 1798.140(q)) personal information on behalf of the business. *See* also FAQ 9: HOW DOES CCPA APPLY TO A SERVICE PROVIDER THAT PROCESSES PERSONAL INFORMATION FOR A CCPA-COVERED BUSINESS?.
[57] Cal PEN CODE § 1546 et seq. The California Electronic Communications Privacy Act applies to California governmental agencies (including law enforcement) that collect electronic communications information..
[58] “Research” is a defined term. CAL. CIV. CODE § 1798.140(s).
[59] CAL. CIV. CODE § 1798.130(a).
[60] CAL. CIV. CODE § 1798.120(c).
[61] "Homepage" means “introductory page of an Internet website and any Internet web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, “About,” “Information,” or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.145 [sic], including, but not limited to, before downloading the application.” CAL. CIV. CODE § 1798.140(l).
[62] CAL. CIV. CODE § 1798.135(b).
[63] CAL. CIV. CODE § 1798.135(a)(2)(B).
[64] CAL. CIV. CODE § 1798.120(d).
[65] *Id.*
[66] *Id*.
[67] CAL. CIV. CODE § 1798.120(d).
[68] 15 U.S.C. §§ 6501–6506.
[69] The FTC interprets “website or online service” broadly to mean “any service available over the Internet or that connects to the Internet or a wide-area network.” COPPA's definition applies not only to websites and mobile applications, but also to plug-ins, widgets, advertising networks and voice over Internet protocol, or VOIP, services. The FTC interprets “website or online service” broadly to mean “any service available over the Internet or that connects to the Internet or a wide-area network.” *See* Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, Question 9.
[70] Under COPPA, several factors are considered, including the digital service's subject matter, visual and audio content, the use of animated characters or other child-oriented activities and incentives, the age of models or celebrities who appeal to children, as well as other reliable evidence about the composition of the actual or intended audience. 15 U.S.C. § 6502(b).
[71] 15 U.S.C. § 6502(b).

©2005-2026 K&L Gates LLP. All Rights Reserved.

[72] CAL.CIV. CODE §1798.125.
[73] *Id.*
[74] CAL.CIV. CODE §1798.125(b)(1).
[75] CAL.CIV. CODE §1798.125(b)(3).
[76] CAL.CIV. CODE §1798.185(b).
[77] CAL.CIV. CODE §1798.140(t)(1).
[78] *Id.*
[79] CAL.CIV. CODE §1798.140(t)(2)(A).
[80] CAL.CIV. CODE §1798.140(t)(2)(B).
[81] CAL.CIV. CODE §1798.140(t)(2)(C).
[82] CAL.CIV. CODE §1798.140(t)(2)(D). CCPA reminds businesses that other changes to a privacy policy also may require advance notice, consistent with California's consumer protection law. *Id.*
[83] “Device” is defined at CAL.CIV. CODE §1798.140(j) as “any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.”
[84] CAL.CIV. CODE §1798.140(d)(1)-(7).
[85] CAL.CIV. CODE §1798.140(d).
[86] CAL.CIV. CODE §1798.140(y). CCPA uses the phrase “verifiable request from the consumer” in certain sections (e.g., §§1798.105(c), 110(b), 115 (a)(3)(b)) which presumably has the same meaning as the defined term “verifiable consumer request.”
[87] CAL.CIV. CODE §1798.130(a)(1).
[88] *Id.*
[89] CAL.CIV. CODE §1798.130(b).
[90] CAL.CIV. CODE §1798.130(a)(2).
[91] *Id.*
[92] CAL.CIV. CODE §1798.185(a)(7).
[93] CAL.CIV. CODE §1798.185(a)(7).
[94] CAL.CIV. CODE §1798.130(a)(2).
[95] CAL.CIV. CODE §1798.140(v).
[96] CAL.CIV. CODE §1798.140(v), 140(w)(2).
[97] CAL.CIV. CODE §1798. 140(w)(2).
[98] CAL.CIV. CODE §1798. 140(w)(2).
[99] CAL.CIV. CODE §1798.140(h). As noted above, personal information is de-identified only if cannot be directly or indirectly linked to a particular consumer and re-identification is prevented by technical and business processes.
[100] “Aggregate consumer information” is information that relates to a group or category of consumers, from which individual consumer identities have been removed and is not reasonably linkable to a consumer, household or device. §1798.140(a).
[101] CAL.CIV. CODE§1798.145(a)(1)-(6).
[102] CAL.CIV. CODE §1798.145(b).
[103] CAL.CIV. CODE §1798.150(a).
[104] CAL.CIV. CODE §1798.155(a).
[105] CAL.CIV. CODE §1798.155(a) (citing Section 17206 of the Business and Professions Code).

©2005-2026 K&L Gates LLP. All Rights Reserved.

[106] CAL.CIV. CODE §1798.155(b).
[107] CAL.CIV. CODE §1798.150(a)(1).
[108] CAL.CIV. CODE §1798.150(a)(2).
[109] CAL.CIV. CODE §1798.150(b)(1).
[110] *Id.*
[111] *Id.*
[112] CAL.CIV. CODE §1798.150(b)(3).
[113] CAL.CIV. CODE §1798.150(b)(2)-(3).
[114] See Note 21.
[115] CAL.CIV. CODE §1798.140(q), GDPR Article 4(8).
[116] GDPR Article 4(1).
[117] CAL.CIV. CODE §1798.140(x).
[118] CAL.CIV. CODE §1798.140(o).
[119] GDPR Article 4(1).
[120] CAL.CIV. CODE §1798.140(q),. GDPR Article 4(2).
[121] GDPR Chapter III.
[122] CAL.CIV. CODE §1798.140(q), GDPR Article 28.
[123] CAL.CIV. CODE §1798.155(a) (citing Section 17206 of the Business and Professions Code).
[124] CAL.CIV. CODE §1798.155(b).
[125] GDPR Articles 83(4).
[126] GDPR Articles 83(5).

KEY CONTACTS



JENNY B. SNEED
PARTNER

RALEIGH
+1.919.743.7323
JENNY.SNEED@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.