THE CCPA: CALIFORNIA CONSUMER PRIVACY ACT

WHAT AGENCIES NEED TO KNOW

4A's | VENABLE LLP

A JOINT PUBLICATION OF THE 4A'S AND VENABLE LLP

About 4A's

The 4A's, founded in 1917, is the leading authority representing the marketing communications agency business. It provides leadership, advocacy and training that empowers agencies to innovate, evolve and grow. It serves 600+ member agencies across 1,200 offices that control more than 85% of total U.S. advertising spend.

The 4A's is committed to protecting the best interests of its members, their employees and the industry at large. Its Benefits division insures more than 164,000 agency professionals, and the D.C. office advocates for policies that best support a thriving advertising industry.

With its best-in-class learning and career development programs, 4A's and its Foundation fuel a robust diversity pipeline of talent for its members and the marketing and media industry, fostering the next generation of leaders.

VENABLE LLP

About Venable LLP's eCommerce, Privacy, and Cybersecurity Team

Venable offers full-service solutions to everything from routine to novel privacy and cybersecurity challenges. Our team brings to bear significant experience and industry knowledge to help clients satisfy data privacy and security laws and maximize their business potential.

Fully immersed in all aspects of data privacy, cybersecurity, and information governance, Venable is unique among privacy and cybersecurity practices. We participate in legislative advocacy, rulemakings, and development of new legal standards. Our team advises organizations with regard to industry best practices and drafting codes of conduct and standards, helping them stay compliant with federal, state, international, and self-regulatory requirements. We provide proactive counseling to guide clients through the potential risks and liabilities associated with corporate transactions. And if government enforcement actions or litigation arise, Venable vigorously defends our clients, mounting challenges to agency regulations and litigating privacy issues and class-action lawsuits.

We strengthen the integrity of our client's data, ecommerce security, and customer or user records; develop internal data collection and use practices; and ensure the creation of sound privacy policies and procedures. We shepherd clients through data-security incidents, and privacy and consumer protection matters, and represent them in connection with corresponding litigation and government enforcement actions. We build and lead coalitions and self-regulatory efforts, and represent leading trade associations in the space.

On **January 1, 2020**, a sweeping new data privacy law will go into effect in the United States. The law, known as the California Consumer Privacy Act (CCPA), is the first of its kind in the country. The CCPA grants California consumers new rights to know about, access, delete, and opt out of the sale of personal information businesses maintain about them, and it imposes requirements on businesses to help fulfill the consumer rights the law creates.

The 4A's offers this primer to agency management, in-house counsel, advertising executives, and others who operate in California or who interact with the personal information of California consumers. This primer seeks to provide an overview of the CCPA, the new rights and requirements it creates, and practical tips for agencies in structuring processes, policies, and contracts to comply with the law. We invite you to use this primer to guide your compliance exercises.

Agency representatives reading this primer should note that the CCPA's terms may evolve based on potential future amendments to the law, regulations interpreting its provisions, and possibly even a new federal law that could preempt the CCPA altogether. The California Attorney General is preparing regulations that may help to clarify some of the CCPA's more ambiguous terms. The descriptions set forth in this primer are therefore subject to change. Clarifying regulations to be issued by the California Attorney General as well as eventual CCPA enforcement actions will shed light on regulators' interpretations of the law. We recommend that you seek legal advice regarding the ways in which the CCPA may impact you and your business.

Below we provide a summary of the substantive provisions of the CCPA with an eye towards the obligations it may pose on agencies related to the personal information they collect and process, both on behalf of clients and for their own purposes. We also provide practical notes and key takeaways along the way in an effort to draw out certain critical parts of the law.

CONTENTS

CHAPTER 1 - THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA): WHAT IT IS, AND WHY IT MATTERS TO AGENCIES

I: CCPA: WHAT IT IS AND WHY IT MATTERS

What is the CCPA?

The CCPA is a far-reaching state data privacy and security law. It creates new rights for California consumers to access, delete, and opt out of the "sale" of the personal information businesses collect about them. The CCPA also creates new obligations for the businesses that collect such consumers' personal information. The law will become operative on January 1, 2020, but its broad scope and novel terms make it necessary for agencies to prepare for its effective date now.

Why does the CCPA matter to agencies?

It is easy to fall within the law's scope. The CCPA defines three categories of entities: businesses, which are directly regulated by the law; service providers, who process information on behalf of a business pursuant to a written contract; and third parties, who are entities that do not collect personal information from consumers directly or receive personal information from a business for a business purpose pursuant to a written contract with terms limiting use, retention, and disclosure.

- *Note* that while the CCPA definition of business is broad, the definition of service provider is limited. Consequently, it is a low threshold for an agency to become a directly regulated *business* under the law.

Even if not directly regulated as a business by the CCPA, agencies can be indirectly impacted. One of the rights the CCPA provides to California consumers is that they may opt out of a business's ability to sell their personal information. "Sale" is defined broadly as any transfer of consumer personal information from a business to another business or a third party for monetary or *other valuable consideration*.

Practical Notes:

- The CCPA's opt-out right limits the availability of personal information in the market to engage in online and offline targeting for advertising campaigns.
- The CCPA imposes requirements on agencies that hold their clients' personal information during a campaign. Even if not directly regulated, agencies may have to assist their clients in complying with CCPA requests if such clients pass the requests through to the agencies.

Covered agencies will have to build compliance mechanisms to facilitate the rights the CCPA creates. Because the CCPA creates new consumer rights, agencies should ensure they have implemented compliance mechanisms to facilitate those rights. As a result, agencies may have to establish and maintain methods for receiving and responding to consumer access, deletion, and opt-out requests. Agencies may also have to update their outward-facing privacy policies to ensure they cover all of the disclosures required under the CCPA.

Running afoul of the CCPA's terms may subject agencies to regulator penalties and private lawsuits. Violating any provision of the CCPA may subject an agency to civil penalties from the California Attorney General. But the California Attorney General is not the only entity that can take action against an agency for violating the law. If an agency runs afoul of the CCPA's data security provisions, it could also be subject to a private lawsuit or class action lawsuit for injunctive relief and damages.

Key Takeaways:

- Although agencies may be service providers under the CCPA in some instances, it is also possible that an agency that deals in California consumers' personal information will be a directly regulated business under the law.
- The CCPA's private right of action opens agencies up to additional penalties outside of those available through regulator enforcement, which can add up in the event of a class action lawsuit.

II: CCPA APPLICABILITY

The CCPA directly applies to a business, as that term is defined under the law.

What is a business? A "business" is defined as a for-profit legal entity that:

- Does business in the state of California;
- Collects California consumers' personal information, or on the behalf of which such information is collected;
- Alone or jointly with others determines the purposes and means of the processing of California consumers' personal information; *and*
- Satisfies at least one of the following thresholds:
  - Has annual gross revenues greater than 25 million dollars;
  - Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more California consumers, households, or devices; or
  - Derives at least 50% of its annual revenues from selling California consumers' personal information.

Additionally, any entity that *controls or is controlled* by a business and that *shares common branding* with the business is part of that single business under the CCPA.

- Control means the power to exercise a controlling influence over the management of a company, including ownership of or the power to vote more than 50% of the outstanding shares of any class of voting security of a business, *or* control in any manner over the election of a majority of the directors or other individuals exercising similar functions for the company.
- Common branding means a shared name, service mark, or trademark.

What is personal information?

Personal information is a broad term that encompasses any information that is capable of being associated with or could reasonably be linked with a particular consumer or household. Personal information includes:

- **Identifiers** such as name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, Social Security Number, driver's license number, passport number, or other similar identifiers
- **Signatures**
- **Physical characteristics or descriptions**
- **Telephone numbers**
- **Characteristics** of protected classifications under California or federal law
- **Insurance policy numbers**
- **Medical information** or **health insurance information**
- Bank account numbers, credit card numbers, debit card numbers, or **any other financial information**
- **Commercial information**, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies
- **Biometric information**
- **Internet or other electronic network activity information**, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement
- **Geolocation data**
- **Audio, electronic, visual, thermal, olfactory, or similar information**
- **Professional or employment-related information**
- **Education information**
- **Inferences** drawn from any personal information to create a consumer profile reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

Personal information does not include "publicly available" information, as that term is defined under the CCPA. "Publicly available" information is carved out from the definition of personal information. However, the term "publicly available" is uniquely defined. It means information that is lawfully made available from federal, state, or local government records *so long as* such information is used for a purpose that is compatible with the purpose for which the data is maintained and made available in public records.

Practical Note:

The purpose limitation in the CCPA's definition of "publicly available" limits the applicability of the term. Information will be considered publicly available, and therefore not personal information, *only if* it is used for a purpose that is in line with the purpose for which the government keeps the information and makes it available for public access.

The CCPA applies to both online and offline data. The CCPA is applicable to data collected online and offline; for example, data collected at a cash register, through in-person contacts, email, websites, applications, or postal mail can be considered personal information under the CCPA.

The CCPA could trigger compliance obligations even if an agency has a single data point on a California consumer. The CCPA does not require an agency to maintain much personal information on California residents to be subject to the law. For example, if an agency does (even limited) business in the state, collects only one point of personal information about a California consumer, determines the purposes and means of processing that data point, and has annual gross revenues in excess of 25 million dollars, the agency may be a directly regulated business under the CCPA.

Practical Note:

The CCPA will impact large and small businesses. Even if an agency and its clients only minimally touch Californians' personal information, the agency could be directly regulated or, at the very least, impacted by the law.

The CCPA may cover an agency even if it has no offices in California. Brands and agencies in the marketing ecosystem may be directly regulated by the CCPA even if they do not maintain a physical presence in California. The CCPA applies to the personal information of California consumers. As a result, if an agency collects or processes California consumers' personal information, it could be subject to the law even if it has no brick and mortar office in the state.

The CCPA contains certain exceptions that may apply to agencies. Notably, in addition to other exceptions, the obligations imposed on an agency by the CCPA may not restrict the agency's ability to:

- Comply with federal, state, or local laws;
- Comply with civil, criminal, or regulatory inquiries, investigations, subpoena, or summons from federal, state, or local authorities;
- Cooperate with law enforcement agencies concerning conduct if the agency reasonably believes the conduct violates the law;
- Exercise or defend legal claims;
- Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information; and
- Collect or sell a consumer's personal information if every aspect of the commercial conduct takes place wholly outside of California. Commercial conduct takes place wholly outside of California if the agency collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information took place in California, and no personal information collected while the consumer was in California is sold.

Furthermore, the CCPA does not require an agency to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

The CCPA also exempts personal information that is governed by separate statutes. For example, the CCPA does not apply to personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, the California Financial Information Privacy Act, or the Driver's Privacy Protection Act. Additionally, the CCPA also does not apply to the following: medical information and providers of health care governed by the Confidentiality of Medical Information Act; and covered entities or health information collected by covered entities or business associates governed by the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and U.S. Department of Health and Human Services privacy, security, and breach notification rules under HIPAA and HITECH.

III: SERVICE PROVIDERS AND THIRD PARTIES

Applicable Statutory Provisions: Cal. Civ. Code § 1798.105; § 1798.115; § 1798.120; § 1798.140.

Businesses are entities that are directly regulated by the CCPA. But the CCPA also defines two other categories of entities that are impacted by the law: service providers and third parties. If an agency meets the definition of a business, it will have particular responsibilities with respect to how it manages the personal information it shares with service providers and third parties. Conversely, if an agency meets the definition of a service provider or a third party, it will have particular responsibilities with respect to how it manages the personal information it receives from businesses. The chart below summarizes these responsibilities.

CCPA Entity	Definition	Business Responsibilities with Respect to the Entity	Entity Responsibilities with Respect to the Business
Service Provider	A for-profit legal entity that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract. The written contract must prohibit the entity receiving the personal information from retaining, using, or disclosing it for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by the CCPA.	A business that receives a deletion request from a California consumer must direct any service providers to also delete the consumer's personal information from their records.	A service provider is not required to delete personal information if it is necessary for the service provider to maintain it for certain select purposes enumerated in the CCPA. Contractual terms between a service provider and a business may obligate the service provider to assist in facilitating access or other consumer requests under the CCPA.
Third Party	A person who is *not* the business that collects personal information from consumers or a person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract that restricts the use, retention, and disclosure of personal information.	A business must refrain from selling personal information to third parties if a consumer opts out of such sale.	A third party may not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out.

Contracts between a business and service provider must include certain terms. To ensure an entity is a service provider, the contract between the service provider and the business must ban the service provider from retaining, using, or disclosing the personal information it receives from the business for any purpose other than for performing the services specified in the contract, or as otherwise permitted by the CCPA.

Furthermore, because the CCPA imposes new requirements on businesses and the way they must handle and manage consumer personal information, such businesses may enlist the help of their service providers in facilitating consumer requests via contractual arrangements. Service providers should take note of any terms to this effect in their contracts with businesses.

Practical Note:

Regardless of whether an agency is a service provider or a business under the law, it is important to pay attention to the ways in which contracts could augment CCPA responsibilities. Negotiating teams should be knowledgeable of the CCPA when engaging in contract reviews and should have a clear understanding of the ways in which contractual language may impose additional CCPA-related obligations on parties.

What constitutes a business purpose? A business purpose is the use of personal information for a business or service provider's operational purposes, or other notified purposes, as long as such use of personal information is reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.

Is the entity a Service Provider? Or is it a Third Party?

Your client has asked you to set up a campaign to generate new customer leads and awareness about its products. You outsource the hosting of the campaign website to a third party web hosting vendor. During the course of the campaign, the web hosting vendor may receive certain consumer personal information from California consumers as it helps effectuate the campaign. If the web hosting vendor is a *for profit entity*, you disclose consumer personal information to the vendor for a *business purpose pursuant to a written contract*, and the written contract *prohibits the web hosting service from retaining, using, or disclosing the consumer personal information it receives from you* for any purpose other than the specific purpose of performing the web hosting services specified in the contract, the vendor is your **service provider** under the CCPA.

After the campaign, your client wishes to share the leads that were generated and the data that was collected with non-affiliated third parties through a data cooperative arrangement. Any non-affiliated third parties that receive lead information are **third parties** under the CCPA.

What constitutes explicit notice? Under the CCPA, third parties who receive personal information from a business may only sell that personal information if the consumer is given explicit notice of the sale and an opportunity to opt out. However, explicit notice is not defined in the CCPA.

Practical Note:

The lack of a definition of explicit notice creates practical difficulties for third parties, who often do not have a direct relationship with the consumer. Providing explicit notice to the consumer and an opportunity to opt out of the sale may be challenging for third parties in the absence of a consumer-facing business model. Agencies should consider addressing this explicit notice requirement in the agreements they maintain with businesses selling data. Agencies may choose to contractually require that such businesses provide the required explicit notice to consumers.

IV: CONSUMERS' RIGHT TO ACCESS

Applicable Statutory Provisions: Cal. Civ. Code § 1798.100; § 1798.110; § 1798.115; § 1798.130; § 1798.140; § 1798.145.

Consumers have the right to access personal information that businesses have collected *about* them. When a business receives a verifiable consumer request, a business must provide the consumer with a list of:

- The specific pieces of personal information a business has collected about them;
- The categories of the personal information a business has collected about them;
- The categories of sources from which the personal information was collected;
- The business or commercial purpose for collecting or selling the personal information; and
- The categories of third parties with whom the business shares personal information.

Additionally, if a business has sold (or disclosed for a business purpose) a consumer's personal information, the business must also provide the consumer with a list of the categories of:

- The personal information that the business sold about them;
- The third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold; and
- The personal information the business has disclosed about them for a business purpose.

If a business has not sold (or disclosed for a business purpose) a consumer's personal information, it must disclose this in its response. A response must cover the 12-month period preceding the consumer's request.

What constitutes a verifiable consumer request? A verifiable consumer request is a request made by a consumer, or by a consumer on behalf on their minor child, or by a person authorized by a consumer to act on their behalf, and that the business can reasonably verify, pursuant to regulations adopted by the California Attorney General.

- ▶ *Note* that businesses must take steps to determine whether a request is a verifiable consumer request, but this process does not extend the time allotted to respond to a request.

When can a consumer make a request? A consumer can make a request that a business provide this information at any time. However, a business is not required to comply with a request from an individual more than twice within a 12-month period.

What does a business have to do to facilitate consumer requests? A business must provide a toll-free telephone number and, if the business has a website, a website address for consumer requests.

How long does a business have to respond? A business must disclose and deliver the required information within 45 days of receiving the request. The time period can be extended an additional 45 days "when reasonably necessary" or up to 90 additional days "where necessary, taking into account the complexity and number of requests," if the business gives the consumer notice.

Businesses' obligation to provide portable data. Businesses must provide the information responsive to access requests free of charge, by mail or electronically. If provided electronically, the information must be in a readily usable format that allows the consumer to transmit the information freely to other entities without hindrance.

Manifestly unfounded or excessive requests. If a consumer makes manifestly unfounded or excessive requests, in particular because of their repetitive character, a business may charge a reasonable fee or refuse to act on the request if the business gives the consumer notice. The business bears the burden of demonstrating a request is "manifestly unfounded or excessive."

Practical Note:

Businesses are not required to retain information collected for a one-time transaction, unless the business sold the personal information or it retains the personal information as part of its normal business practice.

V: CONSUMERS' RIGHT TO DELETION

Applicable Statutory Provisions: Cal. Civ. Code § 1798.105; 1798.130.

Consumers have the right to request a business delete personal information that the business has collected *from* the consumer. When a business receives a verifiable consumer request to delete a consumer's personal information, it must delete that consumer's personal information from its records and direct any service providers to comply with the deletion request.

Are service providers subject to deletion requests? Businesses have an obligation to direct any service providers to comply with deletion requests they receive. If an agency is acting as a service provider, it will have to comply with deletion requests it receives from its clients.

Are there exceptions? Businesses and service providers may not have to delete consumer personal information if it is necessary for the business or service provider to maintain the personal information for one of the following purposes:

- To complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or perform a contract between the business and consumer;
- To detect security incidents, protect against malicious, deceptive, fraudulent or illegal activity, or prosecute those responsible for that activity;
- To identify and repair errors that impair existing intended functionality;
- To exercise free speech, ensure the right of another consumer to exercise his or her right to free speech, or exercise another right provided for by law;
- To comply with the California Electronic Communications Privacy Act;
- To engage in public or peer-reviewed scientific, historical, or statistical research in the public interest, but only if the consumer has given informed consent and the businesses' deletion of personal information is likely to make the research impossible or seriously impair it;
- To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on their relationship with the business;
- To comply with a legal obligation; or
- To otherwise use the personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

VI: CONSUMERS' RIGHT TO OPT OUT OF SALES

Applicable Statutory Provisions: Cal. Civ. Code § 1798.120; § 1798.135; § 1798.140.

Consumers have the right to opt out of a business's sale of their personal information to third parties. To facilitate consumers' ability to opt out, businesses must provide a clear and conspicuous link titled "Do Not Sell My Personal Information" on their Internet home page, in their privacy policy, and in any California-specific description of consumers' privacy rights.

What constitutes a sale? Under the CCPA, a "sale" is defined as a business selling, renting, releasing, disclosing, disseminating, making available, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to another business or a third party for monetary *or other valuable consideration.*

Are there exceptions to the definition of a sale? A transaction is not considered a sale under the CCPA if it meets one of the following exceptions:

- A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information (unless the sale is permitted under the CCPA);
- The business uses or shares a consumer identifier for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information;
- The business uses or shares a consumer's personal information with a service provider, that is necessary to perform a business purpose, if:
  - the business has provided notice that information is being used or shared in its terms and conditions; and
  - the service provider does not further collect, sell, or use the personal information except as necessary to perform the business purpose.
- The consumer's personal information is transferred by a business to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business.

Use of an authorized agent: A consumer may authorize an agent to opt out of the sale of their personal information on their behalf. Businesses must comply with an opt-out request received from a consumer's authorized agent.

Applicability to third parties: A third party may not sell personal information about a consumer that has been sold to it by a business unless the consumer has received explicit notice and is provided an opportunity to opt out of the sale.

What happens after a consumer opts out? Once a consumer opts out, businesses must refrain from selling that consumer's personal information to third parties. Businesses must wait at least 12 months before requesting that a consumer who opted out authorize the sale of that consumer's personal information.

Practical Note:

Businesses may only use personal information collected from a consumer in connection with an opt-out request for the purposes of complying with the request.

VII: CONSUMERS' RIGHT TO KNOW/TRANSPARENCY OBLIGATIONS

Applicable Statutory Provisions: Cal. Civ. Code § 1798.100; § 1798.110; § 1798.130; § 1798.135.

Under the CCPA, businesses must notify consumers of their rights under the law and ensure that employees are prepared to handle CCPA requests. To meet these requirements, businesses must make certain disclosures to consumers.

Disclosures "at or before" the point when personal information is collected. A business that collects personal information must, "at or before the point of collection," inform consumers of:

- A list of the categories of personal information the business will collect; and
- The purposes for which the categories shall be used.

A business may not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice. These disclosures must be made in a "form that is reasonably accessible to consumers," such as a business's privacy policy or website.

Privacy policy disclosures. The CCPA also requires businesses to make certain disclosures in their privacy policies and in any California-specific description of consumers' privacy rights. Businesses must update these disclosures at least once every 12 months. Businesses must disclose the following:[1]

- A description of:
  - one or more designated methods for submitting CCPA requests to the business, such as a toll-free number and website address.
  - the rights afforded to California consumers under the CCPA.
  - the business obligation not to discriminate against consumers for exercising CCPA rights.
- A list of:[2]
  - the categories of personal information the business collected about consumers.
  - the categories of sources from which the business collected personal information about consumers.
  - the categories of third parties with whom the business shared personal information.
  - the categories of personal information the business has sold about consumers.
    - If the business has not sold consumers' personal information in the preceding 12 months, the business must disclose that fact.
  - the categories of personal information the business has disclosed about consumers for a business purpose.
    - If the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business must disclose that fact.
  - the specific pieces of personal information the business has collected about that consumer.
  - the business or commercial purposes for collecting or selling personal information.
- A link to the "Do Not Sell My Personal Information" webpage.

[1] The CCPA does not clearly identify all of the disclosures that are required, and the California Attorney General's regulations may clarify this requirement in the future. Given the lack of clarity, this primer is over-inclusive, based on the plain language of the CCPA.

[2] Each of these items must contain responsive information for the preceding 12 months.

Employee training. Though the CCPA imposes no explicit employee training requirements, the law generally requires a business to ensure that the employees who handle consumer inquiries about the business's privacy practices or the CCPA are informed of the CCPA's requirements and how to direct consumers to exercise their rights.

"Do Not Sell My Personal Information" link. Businesses must provide a clear and conspicuous link on their Internet homepage, in their privacy policies, and in any other California-specific description of consumers' privacy rights titled "Do Not Sell My Personal Information." Businesses must give consumers the ability to click on this link to opt out of the sale of their personal information.

- ▶ *Note* that a business cannot require a consumer to create an account with the business in order to place a request with the business not to sell the consumer's personal information.

Practical Note:

As indicated above, the CCPA sets forth a 12-month look-back period that requires a business to disclose the categories of consumer personal information it collected in the prior 12 months. Additionally, the CCPA establishes a 12-month look-back period with respect to consumer access requests to which businesses must respond. As a result, agencies should develop processes that enable them to: (1) ascertain the categories of consumer information they collected over the prior 12-month period; and (2) identify and provide specific pieces of information they collected about a consumer over the prior 12-month period.

Key Takeaways:

- Businesses must disclose which categories of personal information they will collect at or before the time of collection and the purpose of this collection. If a business collects additional personal information not previously disclosed or for another purpose not previously disclosed, it must notify consumers.
- Businesses are required to make certain disclosures in their privacy policies. The California Attorney General may clarify the privacy policy disclosures that are required through regulations.
- While the CCPA imposes no specific employee training requirements, business employees who will interface with consumers should be aware of CCPA rights and how to direct consumers to effectuate them.
- Businesses should be prepared to append a "Do Not Sell My Personal Information" link to their Internet homepage and privacy policies to enable consumers to opt out of the sale of personal information.

VIII: MINORS' RIGHT TO OPT IN

Applicable Statutory Provisions: Cal. Civ. Code § 1798.120.

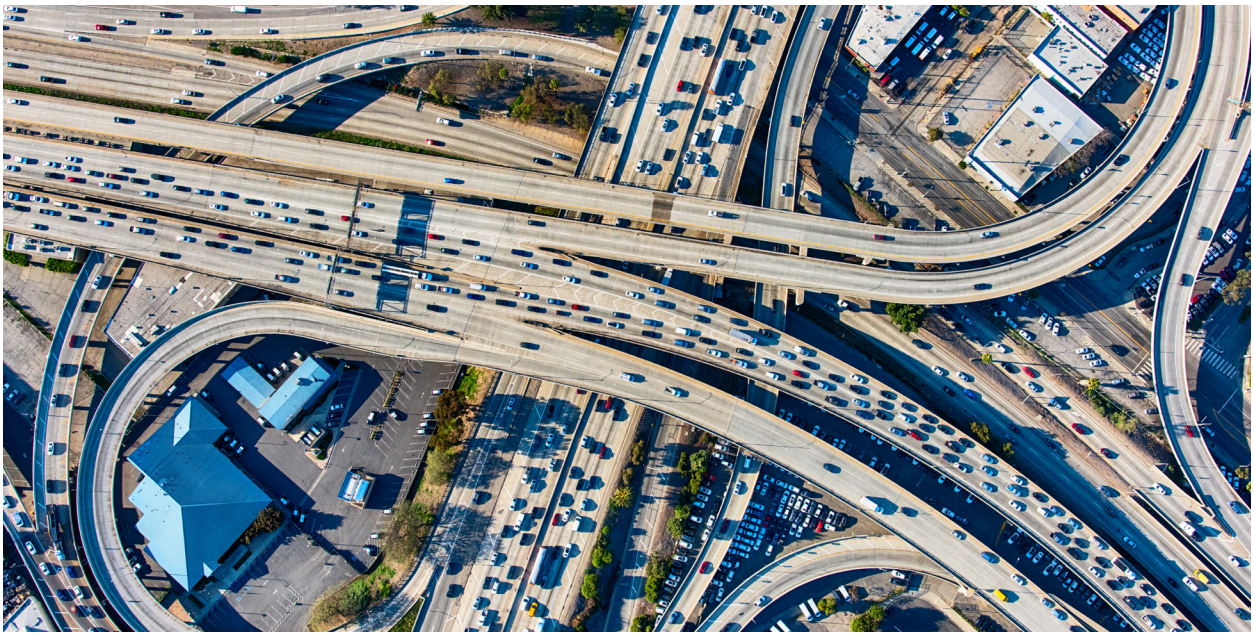
Under the CCPA, individuals under the age of 16 have the right to opt in to the sale of their personal data.

Right to opt in. A business may not sell the personal information of a consumer if the business has *actual knowledge* the consumer is less than 16 years of age, unless the business has received opt-in consent to sell such information. For consumers aged 13 to 15, the consumer must provide such opt-in consent. For consumers under 13 years of age, the consumer's parent or guardian must provide such opt-in consent.

Actual knowledge. The CCPA states that it will impute actual knowledge of a consumer's age to a business that has willfully disregarded the consumer's age.

Practical Notes:

- The Children's Online Privacy Protection Act ("COPPA") applies to minors under age 13, but the CCPA's opt-in right applies to minors under age 16. This means that requirements will apply to 13, 14, and 15 year-olds under the CCPA that do not apply under COPPA.
- Furthermore, under COPPA, a website operator of any website or online service directed to children that collects personal information of children or has actual knowledge it is collecting personal information from a child must obtain verifiable parental consent for the collection, use, or disclosure of personal information from children. COPPA's consent requirements, therefore, are based on a website operator's *actual knowledge* it is collecting personal information from children. But the CCPA *imputes actual knowledge of a minor's age* to a business that has willfully disregarded a minor's age. As a result, agencies should have processes to detect and flag consumers under the age of 16. For example, if an agency collects consumers' birthdates or other information that would indicate age, the agency should have procedures to identify California consumers who must opt in to the sale of their personal information and, if necessary, develop a process for obtaining consent from a parent or guardian.



IX: NONDISCRIMINATION

Applicable Statutory Provisions: Cal. Civ. Code § 1798.125.

Businesses cannot discriminate against consumers for exercising CCPA rights. The CCPA forbids a business from taking retaliatory action against a consumer for exercising his or her rights under the CCPA. Specifically, subject to certain exceptions, a business may not discriminate against a consumer by:

- Denying goods or services to the consumer;
- Providing a different level or quality of goods or services to the consumer;
- Charging a consumer a different price or rate for goods or services, including through discounts, other benefits, or penalties; or
- Suggesting the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services for exercising CCPA rights.

Financial incentive programs. Despite the CCPA's prohibition on discriminating against a consumer for exercising CCPA rights, the law allows businesses to offer financial incentive programs to consumers as compensation for the collection, sale, or deletion of personal information. A business that offers such a financial incentive program must:

- Appropriately notify consumers of the financial incentive, clearly describing the material terms of the program;
- Provide for opt-in consent to the financial incentive; and
- Allow the consumer to revoke his or her consent to participate in the financial incentive program at any time.

Practical Note:

Though the financial incentive program requirements may not directly impact agencies, agencies should be aware of them in case they work on a campaign for a client that includes a financial incentive program, such as a sweepstakes.

X: ENFORCEMENT

Applicable Statutory Provisions: Cal. Civ. Code § 1798.150; § 1798.155.

The California Attorney General may enforce the CCPA by bringing lawsuits for civil penalties against businesses that have violated any provision of the law. Additionally, the CCPA enables private litigants to bring civil actions to obtain statutory damages for a violation of the law's data security provisions. Businesses have an opportunity to cure their alleged violations in the event of a lawsuit from either the California Attorney General or a private litigant. The enforcement terms of the CCPA are summarized in the chart below.

Enforcer	Required Violation	Available Relief/Penalties	Available Cure Period
California Attorney General	Any violation of the CCPA	• Civil penalties in the amount of $2,500 for each violation or $7,500 for each intentional violation; *and* • Injunctive relief.	Yes, a business may avoid civil penalties by curing the violation within 30 days after being notified of alleged noncompliance by the California Attorney General.
Private Litigant or Certified Class	If a business violates its duty to implement and maintain reasonable data security procedures and practices appropriate to the nature of the information, and as a result, the consumer's nonencrypted or nonredacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure.	• The greater of damages in the amount of $100 - $750 per consumer per incident *or* actual damages; • Injunctive *or* declaratory relief; *and/or* • Any other relief the court deems proper.	Yes, upon receiving notice of a violation from a private litigant, a business may avoid penalties by curing the violation within 30 days of the notice, providing the litigant with an express written statement that the violations have been cured, and stating that no further violations shall occur.

Practical Note:

The "personal information" that must be exposed to enable a consumer to file a private lawsuit, as described on page 10, is *narrower* than the CCPA's definition of the term "personal information." A consumer may bring a private right of action only if the following "personal information" is subject to unauthorized access and exfiltration, theft, or disclosure: an individual's first name or first initial and his or her last name *in combination with* the individual's Social Security Number; driver's license number or California identification card number; account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to the individual's financial account; medical information; or health insurance information.

CHAPTER 2 – CCPA COMPARED TO GDPR

I: COMPARISON CHART

On May 25, 2018, the General Data Protection Regulation ("GDPR") went into effect in the European Union ("EU"), and on January 1, 2020, the CCPA will become operative in California. These two wide-ranging data privacy laws have already had significant implications for entities that operate in both the United States and the EU.

While the CCPA generally allows consumers to *opt out* of the sale of their personal information, the GDPR requires *opt in* consent. The GDPR explicitly states that silence, pre-ticked boxes, or inactivity does not constitute consent, thereby requiring consumers to affirmatively opt in to data processing under the law.

Below we provide a chart comparing other important facets of the CCPA and the GDPR. The main topic areas addressed are information that is covered by the laws, entities that are covered by the laws, notice requirements, and individual rights and controls under each of the laws.

- *Note* that the chart does not cover every obligation imposed by the CCPA and GDPR, but rather highlights key areas where the laws overlap and where they diverge.

Topic Area	CCPA	GDPR
Information Covered by the Laws	**"Personal information"** is any 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. A **"consumer"** is a California resident.	**"Personal Data"** is any information that is related to an identified or identifiable natural person. Persons are **"identifiable"** if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. The GDPR refers to individuals in the EU as **"data subjects."**
Entities Covered by the Laws	**"Businesses,"** which are: (1) for-profit entities that do business in California and collect Californians' personal information *if*: they have annual revenues in excess of $25 million; annually buy, receive, sell, or share for a commercial purpose the personal information of 50,000 or more California consumers, households, or devices; or derive at least half of their annual revenues from selling consumer personal information, and (2) any entity that controls or is controlled by a business and shares common branding with that business.	**"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. **"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Topic Area	CCPA	GDPR
Entities Covered by the Laws *continued*	**"Service providers,"** which are for-profit entities that process information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, so long as the written contract contains certain terms limiting the service provider's ability to use, retain, and disclose the information. **"Third parties,"** which are *not*: businesses that collect personal information from consumers, or persons to whom businesses disclose a consumer's personal information for a business purpose pursuant to a written contract.	**"Processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Privacy Policy / Notice Requirements	The CCPA requires that businesses inform consumers of the categories of personal information collected and the uses of such personal information *at or before the point of information collection*. Such notice may be given in a privacy policy or other California-specific description of consumers' privacy rights. The required privacy policy disclosures are as follows: • A description of the methods for submitting CCPA requests; • A description of California consumers' CCPA rights; • A description of the business obligation to refrain from discrimination against consumers for invoking CCPA rights; • A list of the categories of personal information the business collected about consumers in the last 12 months; • A "Do Not Sell My Personal Information" link; • A list of the categories of sources from which the personal information about consumers was collected in the last 12 months; • The business or commercial purposes for collecting or selling personal information in the last 12 months;	Under the GDPR, companies must provide an *easily accessible, concise notice* to individuals about the processing of their Personal Data. The notice must contain the following information: • The identity and contact information for the company, the company's representative, and the company's data protection officer (if applicable); • A description of individuals' GDPR rights; • The categories of information processed and the source of the information (if not collected directly from the individual); • The recipients of information, and information regarding the transfer of information to international locations or organizations; • The purposes for the processing of such information and the legal basis for the processing, in addition to the legitimate interests of the entity processing the data; • The amount of time for which the information is retained.

Comparison chart continued.

Topic Area	CCPA	GDPR
Privacy Policy / Notice Requirements *continued*	• A list of the categories of third parties with whom the business shared personal information in the last 12 months; • A list of the specific pieces of personal information the business has collected about that consumer in the last 12 months; • A separate list of the categories of personal information the business has sold about consumers in the last 12 months (or, if it has not sold personal information, a statement to that effect); and • A separate list of the categories of personal information the business has disclosed about consumers for a business purpose in the preceding 12 months (or, if it has not disclosed personal information, a statement to that effect).[2]	
Consumer / Individual Rights and Controls	The CCPA gives consumers the following rights: • Right to access; • Right to deletion; • Right to opt out of the sale of personal information to third parties; • Right to know and receive certain disclosures from a business; and • Right to opt in to the sale of personal information to third parties (for minor consumers under the age of 16). The CCPA also places obligations on businesses that may implicate certain consumer entitlements: • If a business provides data to consumers electronically, such data must be portable and in a readily usable format that allows the consumer to freely transmit it without hindrance; and • A business may not discriminate against consumers for exercising their CCPA rights.	The GDPR gives EU individuals the following rights: • Right to access; • Right to erasure (i.e., the right to be forgotten); • Right to restriction of processing; • Right to rectification; • Right to data portability • Right to object; and • Right to be free from automated decision-making.

[2] *The CCPA's privacy policy requirements may be further clarified when the California Attorney General issues regulations interpreting the law.*

Practical Notes:

- The CCPA's right to deletion is slightly different from the GDPR's right to erasure. The GDPR right to erasure applies only in 6 particular circumstances such as when the individual withdraws consent to their continued data processing; requests that do not meet one of these enumerated circumstances do not have to be fulfilled. On the other hand, the CCPA right to deletion allows any California consumer to request the deletion of personal information collected from them by the business. Despite the broad availability of the right to consumers, the CCPA has exceptions for businesses complying with the right that the GDPR does not offer. For example, if a business needs to maintain the consumer's information to enable internal uses that are reasonably aligned with the expectations of the consumer, the business is not required to delete the consumer's personal information. The GDPR does not include such an exception to the right to erasure.
- Agencies that have adjusted their internal policies and practices to comply with the GDPR may have a head start on work needed for CCPA compliance. Agencies should consult with legal counsel to ascertain areas where they can leverage GDPR compliance mechanisms for CCPA purposes.

CHAPTER 3 – CCPA IMPLEMENTATION

I: TIMELINE

Keep these key dates in mind with respect to CCPA enforcement and potential changes to the law.

January 8, 2019-March 5, 2019: The CCPA requires the California Attorney General to solicit public participation and adopt regulations to further the purpose of the CCPA. The California Attorney General must adopt regulations to:

- Update the categories of personal information;
- Update the definition of unique identifiers;
- Establish any exceptions necessary to comply with state or federal law;
- Establish rules and procedures for the following:
  - Facilitate and govern the submission of consumers' opt-out requests and to govern business compliance with consumers' opt-out requests
  - For development and use of a recognizable and uniform opt-out logo
- Adjust the amount of gross revenue required to meet one of the business definition thresholds in January of every odd-numbered year to reflect any increase in the Consumer Price index;
- Establishing rules, procedures, and any exceptions necessary to ensure that notices and information businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings;
- Establishing rules and procedures related to consumers' use of authorized agents and to govern a business's determination that a request for information received by a consumer is a verifiable consumer request.

The Attorney General may also adopt regulations as necessary.

To solicit public participation in the regulatory process, the California Attorney General held a series of seven pre-rulemaking public forums that took place in San Francisco, San Marcos, Riverside, Los Angeles, Sacramento, Fresno, and Stanford.

March 8, 2019: The California Attorney General's Office concluded the public comment period.

What happens after the public comment period? The next step is for the California Attorney General to issue proposed regulations and rules and provide a 45-day opportunity for public comment. Thereafter, if any changes to the rules constitute substantial and sufficiently related changes, the California Attorney General must mail a notice and the text of proposed changes and provide for a public comment period of 15 days. If the rules constitute major changes, the California Attorney General must issue a new proposed rule and provide for a public comment period of at least 45 days.

September 13, 2019: Last day of the legislative session for the California Legislature to pass any amendments to the CCPA.

October 13, 2019: Last day of the year for the California Governor to sign or veto any amendments to the CCPA passed by the California Legislature.

January 1, 2020: CCPA becomes effective.

July 1, 2020: The California Attorney General will begin enforcing the CCPA on this date or 6 months after the publication of the final regulations interpreting the CCPA, whichever comes sooner.

Key Takeaway:

The timeline for CCPA enforcement and updates is evolving. Changes to the CCPA could come in the form of California Attorney General regulations, potential legislative amendments, or in the form of a new federal law. Agencies should continue to closely follow developments in the law.

II: PRACTICES CHECKLIST

Even though the CCPA does not become effective until January 1, 2020, agencies should begin working towards CCPA compliance as soon as possible. For agencies wondering where to begin, here are some suggested activities to help you prepare for the CCPA.

Suggested Tasks

- ☐ **1. Check whether the CCPA applies to your agency.** The CCPA applies to agencies that collect California consumers' personal information, or on the behalf of which such information is collected, doing business in California with:
  - over $25 million in annual gross revenues;
  - that receive or share personal information for 50,000 or more consumers, households or devices; *or*
  - that derive more than half of their annual revenues from consumer data sales.
- ☐ **2. Review the personal data that your agency collects and the purposes for which you use and share this personal data.** This will help your agency determine how to comply with the CCPA. The CCPA has a broad definition of personal information, which captures any information that is capable of being associated with a consumer or household.
- ☐ **3. Start looking back at personal data practices.** Under the CCPA, businesses are required to respond to verifiable consumer requests with information for the 12-month period preceding the request. It is unclear if this provision will require businesses to disclose their personal data practices prior to the CCPA's effective date of January 1, 2020. In light of this, businesses should begin taking stock of their personal data practices as soon as practicable.
- ☐ **4. Assess if your agency shares personal data in a way that could constitute a "sale" under the CCPA.** Under the CCPA, a "sale" is defined broadly as any transfer of personal data in exchange for something of value. If your agency is "selling" personal data, it must allow consumers to opt out.
- ☐ **5. Consider how your agency shares personal data with your affiliates.** A "business" under the CCPA encompasses entities that control or are controlled by the same business and share common branding. Affiliates with different brandings, or that are not a parent or subsidiary company, may be considered separate businesses.
- ☐ **6. Prepare a process to execute access and deletion requests.** Businesses and service providers governed by the CCPA will have to respond to access and deletion requests. Your agency will have to verify the identity of the consumer making the request and if any exceptions are available to exempt your agency from the request.
- ☐ **7. Review contracts and public disclosures.** If your agency employs service providers, your agency's contracts with these service providers must contain certain provisions. Your agency should identify if it will need to amend existing contracts and should revise any standard contracts. In public disclosures, agencies will be required to provide new notices to consumers, such as informing them about their rights to access, delete, and opt out of sales of their personal information.
- ☐ **8. Assess if your agency collects personal data from consumers under the age of 16.** The CCPA places particular obligations on a business when it collects personal data from consumers under the age of 16. If your agency has actual knowledge a consumer is under the age of 16, your agency may not sell their personal data unless the consumer has provided opt-in consent or parental consent (if the consumer is under 13 years of age).
- ☐ **9. Review your agency's data security practices.** The CCPA grants consumers a private right of action, linked to statutory damages, for consumers who have had their personal information exposed because of security breaches, if such a breach is a result of the business's failure to provide reasonable security. Businesses have 30 days to "cure" any alleged violation.
- ☐ **10. Stay on the lookout for CCPA developments.** Important updates to the CCPA could come in the form of California Attorney General regulations, potential legislative amendments, or a new federal law.

CONTACT US

4As

Dick O'Brien
EVP, Government Relations
dobrien@4as.org

Alison Pepper
SVP, Government Relations
apepper@4as.org

VENABLE LLP

Stu Ingis
Partner
singis@Venable.com

Emilio Cividanes
Partner
ewcividanes@Venable.com

Shannon Yavorsky
Partner
skyavorsky@Venable.com

Mike Signorelli
Partner
masignorelli@Venable.com

Kelly DeMarchis Bastide
Partner
kabastide@Venable.com

Julia Tama
Partner
jatama@Venable.com

Hannah Levin
Associate
hilevin@Venable.com

Allaire Monticollo
Associate
amonticollo@Venable.com