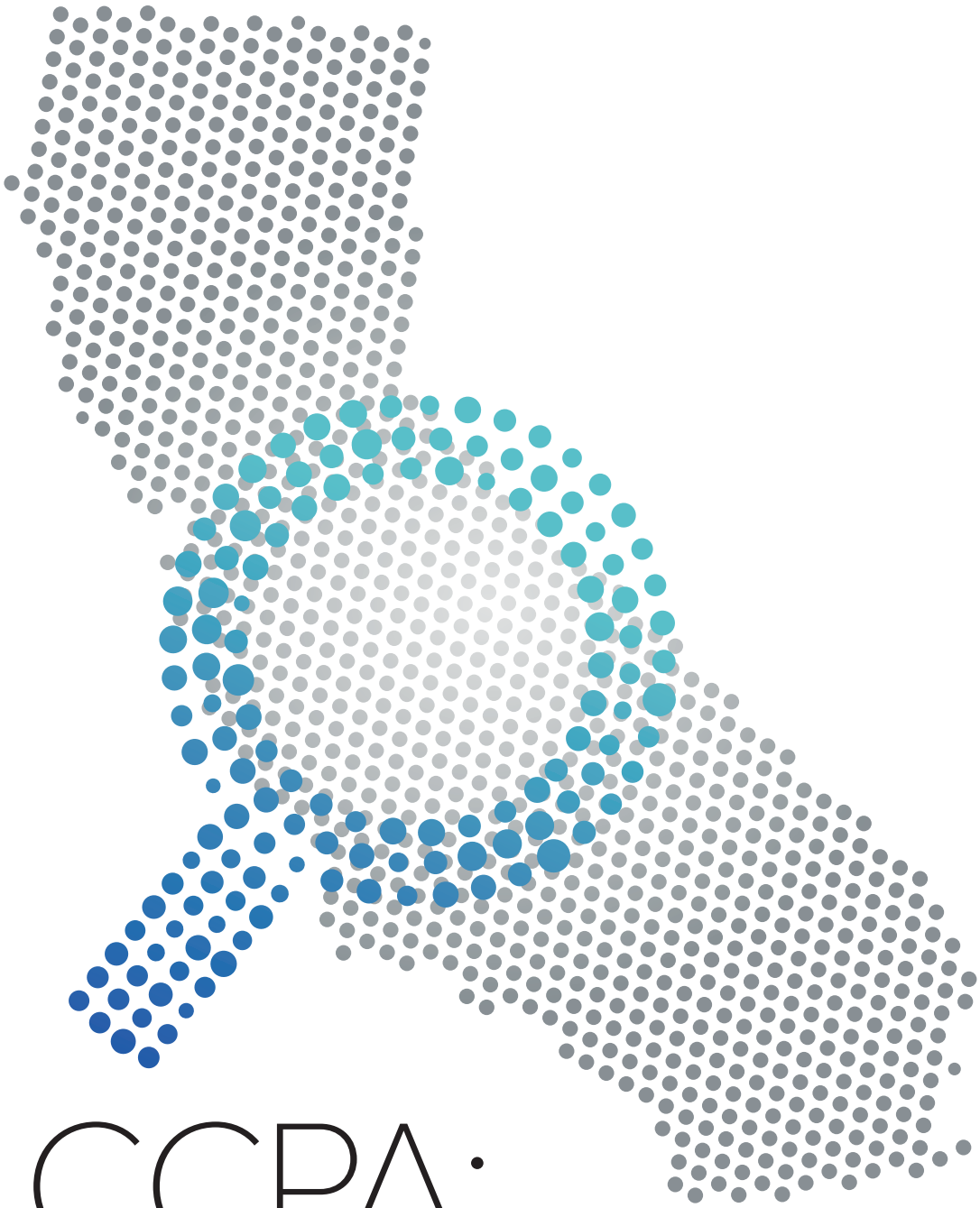
O'Melveny | What do you want to achieve?



CCPA: Client Toolkit

What is the CCPA?

The California Consumer Privacy Act (CCPA) is the State of California's new data privacy law imposing significant obligations on companies with respect to the personal information of California residents. The CCPA took effect on January 1, 2020, with enforcement delayed until July 1, 2020 or six months after issuance of the Attorney General's regulations, whichever is sooner. The Attorney General has made several public statements that the Attorney General's Office will be active in enforcement of these new obligations. Companies subject to the CCPA should promptly examine their personal data collection and processing practices and determine what, if any, changes in practices or documentation that they must make to comply.

THE CCPA IN BRIEF

The CCPA grants California consumers broad rights to control their "personal information," a term defined expansively by this law. The California Legislature passed the CCPA in June 2018 in response to a proposed ballot measure providing even more stringent privacy protections. It has been amended several times since then and is also subject to regulations promulgated by the California Attorney General. Although further amendments or another initiative may occur, even in current form the CCPA imposes major new privacy obligations on businesses.

Effective January 1, 2020, the CCPA will be the strictest privacy law in the nation and will provide new data rights for California residents, including the right to know, obtain, access, and request deletion of their personal information and to say no to the sale of their personal information.

Businesses subject to the law will need to assess what personal information they collect from California residents and will need to implement processes and procedures to comply with CCPA's new requirements and obligations.

According to an **economic impact assessment** prepared for the California Attorney General's Office by an independent firm, the CCPA is projected to have a significant impact on businesses, affecting up to 400,000 California-based businesses alone and resulting in compliance costs of more than $55 billion over the next decade. And the law is not limited to businesses based in California; it affects businesses outside California that collect or use information about California residents.

Given upcoming deadlines, businesses should quickly determine whether they will need to comply with the CCPA and, if so, assess needed operational changes and associated costs of compliance.

In this toolkit, we provide an overview of key CCPA concepts and offer specific steps to consider in working toward CCPA compliance.

The following are some of the key concepts of the CCPA[1]:

Covered Businesses

- The CCPA applies to a "business," which is defined as any for-profit entity doing business in California that collects California consumers' ("consumers" must be permanent California residents) personal information, including a parent or subsidiary of such an entity, which shares common branding and that meets one or more of these thresholds:
  - Gross revenues in excess of $25 million annually;
  - Annually buys, receives, sells, or shares for commercial purposes the personal information of at least 50,000 consumers, households, or devices; or
  - Derives 50% or more of its annual revenues from selling consumers' personal information.
- The definition of a business also includes any entity that controls or is controlled by a covered business and that shares common branding with the covered business. "Controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.
- Non-profit entities are exempt from the CCPA's requirements.

Personal Information

- The 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.
- Publicly available information and de-identified or aggregate consumer information are not personal information under the CCPA. To be "publicly available," information must be lawfully made available from federal, state, or local government records. Publicly available information excludes biometric information collected by a business about a consumer without the consumer's knowledge.
- Examples of personal information covered by the CCPA include:
  - personal identifiers, such as a real name, alias, postal address, unique personal identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
  - biometric information;
  - geolocation data;

[1] The CCPA is codified under CAL. CIV. CODE §1798.100 - 1798.199.

- audio, electronic, visual, thermal, olfactory, or similar information;
- commercial information, such as records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Internet or other electronic network activity information, such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;
- professional, employment-related, and 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;
- characteristics of protected classifications under California or federal law; or
- categories of any personal information that identifies, relates to, describes, or is capable of being associated with a particular individual, including a signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

Consumer Notices and Privacy Policy

- The CCPA requires covered businesses to provide notice to consumers of their privacy practices before collecting the consumer's personal information. The proposed regulations describe the style, content, and format of the required notices to consumers, including notice of data collection practices, the right to opt-out of sale of personal information, financial incentives, and online privacy policies. The following are requirements applicable to all these notices:
  - The proposed regulations provide that any notices should be in straightforward, plain language that avoids technical or legal jargon.
  - The consumer's attention should be drawn to the notice, including the use of formats accessible to those with disabilities and covering all languages in which the business offers contracts in the ordinary course of business, among other requirements.
  - The notice should be provided at or before the collection of personal information; the regulations provide examples of how the notice can be provided in both online and offline scenarios.
  - The proposed regulations detail the notice requirements for the right to opt-out of sale of personal information, including placing "Do Not Sell My Personal Information" or "Do Not Sell My Info" links on the homepage of the business collecting the information.

- Privacy policies must describe a business's practices regarding the handling of personal information and of consumers' rights regarding their personal information. A business's privacy policy must be updated at least once per year and should be posted online through a conspicuous link using the word "privacy" on the business's website homepage (or on the download or landing page of a mobile application). A privacy policy must also follow other specific requirements, such as be available in an additional format that allows a consumer to print it out as a separate document.

Disclosure Obligations

- Under the CCPA, a consumer has a right to request that a business that collects or sells the consumer's personal information disclose to that consumer the details about the personal information the business has collected or sold.
- A business that receives a verifiable disclosure request (described below) from a consumer may be required to disclose information including:
  - the categories and specific pieces of collected personal information;
  - the categories of sources from which the personal information is collected;
  - the business purposes for collecting or selling personal information;
  - the categories of personal information the business sold or disclosed about the consumer for a business purpose; and
  - the categories of third parties with whom the business shared or to whom the business sold personal information about the consumer.
- A business is not obligated to provide those types of information to the same consumer more than twice within a 12-month period.

Verifying and Responding to Consumer Requests

- A "consumer" under the CCPA is a natural person who is a California resident. A California resident is an individual who is in California for other than a temporary or transitory purpose, or who, while domiciled in California, is outside of California for a temporary or transitory purpose. All individuals outside these two groups are nonresidents.
- The CCPA outlines how businesses should verify the identity of account holders and non-account holders who may make requests of the business. A business is required to establish, document, and comply with a reasonable method for verifying that the person making a request is the consumer about whom the business has collected information, and this method should take into account the sensitivity of the information and the risk of harm. According to the proposed CCPA regulations, different verification methods may be implemented depending on whether a consumer has an account with the business.
  - Verification of Account Holders:
    - Businesses that maintain a password-protected account with the consumer may verify the consumer's identity through their existing authentication practices for the consumer's account.

    - Verification of Non-Account Holders:
        - For requests for "categories" of information collected: a "reasonable degree of certainty" is required (i.e., at least two data points of personal information).
        - For requests for specific personal information: a "high degree of certainty" is required (i.e., at least three data points of personal information and a signed declaration with penalty of perjury).
- The deadline for a business to respond and deliver the report free of charge is 45 days from receiving the verifiable consumer request. This deadline may be extended by up to 90 additional days where necessary. The business must inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.
- If the business does not act on the consumer's request, the business must inform the consumer of the reasons for not taking action and of any rights the consumer may have to appeal the decision to the business.
- If requests from a consumer are manifestly unfounded or excessive, a business may either charge a reasonable fee or refuse to act on the request and notify the consumer of the reason for refusing the request. The business bears the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.
- A CCPA amendment passed earlier this year introduces temporary limitations on the types of personal information subject to the CCPA:
    - ***Temporary exception for employees and contractors.*** Until January 1, 2021, a piece of personal information is exempt from most CCPA provisions if it is collected from a natural person by a business in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business. Also exempt is emergency contact information or personal information necessary to administer benefits for another natural person relating to the employee, owner, director, officer, medical staff member, or contractor. However, these individuals retain their rights to be informed of the categories of personal information collected and the purposes for which these categories of personal information shall be used by the business.
    - ***Temporary exemption for certain business-to-business information.*** Until January 1, 2021, a piece of personal information is exempt from most provisions of the CCPA if it reflects a written or verbal communication or a transaction between the business and a person acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency if the communication or transaction occurs solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency. Under this exemption, most email communications between individuals in their roles as employees of businesses would not be subject to CCPA requests.

- Separate from the obligations tied to specific consumer rights, a business subject to the CCPA also incurs certain internal obligations, such as:
  - making available to consumers two or more designated methods for submitting requests for information required to be disclosed by the business pursuant to a consumer's disclosure rights, where the methods include, at a minimum, a toll-free telephone number and, if the business maintains a website, a website address. California Attorney General's proposed CCPA regulations discuss several rules on submission methods, including requiring a business (1) to offer at least one request submission method offered to reflect the manner in which the business primarily interacts with the consumer; (2) to use a two-step process for online deletion requests; (3) to treat either a deficient or incorrectly submitted request as if it had been submitted properly, or to guide the consumer on how to submit the request or remedy the deficiency; and
  - ensuring that all the parties responsible for handling consumer inquiries about the business's privacy practices or the business's CCPA compliance are informed of all the business's obligations and how to direct consumers to exercise their CCPA rights.

Deletion Obligations

- A business must delete a consumer's personal information after receiving a verifiable deletion request from the consumer. Furthermore, a business must honor the consumer's deletion request by asking any companies that process the consumer's personal information on behalf of the business to delete such personal information.
- However, a business can refuse to delete a consumer's personal information if it is necessary for the business to maintain this information to:
  - complete the transaction for which the personal information was collected or otherwise complete a contractual transaction between the business and the consumer;
  - detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity;
  - debug to identify and repair errors that impair existing intended functionality;
  - exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law;
  - comply with select provisions of the California Electronic Communications Privacy Act, which regulates law enforcement's receipt of personal information through warrants and wiretaps;
  - engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when a business's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent;

- enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;
- comply with a legal obligation; or
- otherwise use the consumer's personal information internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

Sales of Personal Information—Opt-out and Opt-in Obligations

- A "sale" under the CCPA means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.
- The CCPA's right to opt out enables a consumer to direct a business, which sells personal information about the consumer, not to sell the consumer's personal information. A business must honor a consumer's opt-out request for at least 12 months before requesting that the consumer reauthorize the sale of the consumer's personal information.
- Additionally, a business may not sell the personal information of children under the age of 16 unless the business obtains affirmative consent from children between the ages of 13 and 16, or from the parent of a child if the child is under the age of 13. In this scenario, children or parents providing affirmative consent are exercising their "right to opt in" under the CCPA.
- The CCPA deems that no sales of personal information occur in the following scenarios:
  - A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party;
  - A business uses or shares an identifier for a consumer who has opted out of the sale of his or her personal information for the purposes of alerting third parties that the consumer has so opted out;
  - A business uses or shares with a service provider consumer's personal information that is necessary to perform a business purpose, so long as (i) the business has provided notice that information being used or shared is consistent with the CCPA opt-out obligations, and (ii) the service provider does not further collect, sell, or use consumer's personal information, except as necessary to perform the business purpose.
  - A business transfers to a third party a consumer's personal information 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, provided that information is used or shared consistently the business's disclosure obligations under the CCPA. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer.

Nondiscrimination Obligation

- A business may not discriminate against a consumer because the consumer exercised any of the consumer's rights under the CCPA. Some examples of discriminatory actions by a business include:
  - denying goods or services to the consumer;
  - providing a different level or quality of goods or services to the consumer;
  - charging the consumer different prices or rates for goods or services, including withholding discounts or other benefits or imposing penalties; or
  - suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
- However, a business may charge a consumer a different price or rate, or provide a different level or quality of goods or services to the consumer, if that difference is reasonably or directly related to the value provided to the consumer by the consumer's data. Other scenarios where this nondiscrimination provision would not apply include where a business offers financial incentives for the collection, sale, or deletion of personal information.
- In its proposed regulations, California Attorney General defines "the value provided to the consumer by the consumer's data" as the value provided to the business by the consumer's data. Hence, in estimating the value of consumer's data, a business offering a financial incentive or a price or service difference to a customer "shall use and document a reasonable and good faith method for calculating the value of the consumer's data." According to the proposed regulations, one or more of the following calculation methods may be used:
  - the marginal or the average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data;
  - revenue or profit generated by the business from separate tiers, categories, or classes of consumers or typical consumers whose data provides differing value;
  - revenue generated by the business from sale, collection, or retention of consumers' personal information;
  - expenses related to the sale, collection, or retention of consumers' personal information;
  - expenses related to the offer, provision, or imposition of any financial incentive or price or service difference;
  - profit generated by the business from sale, collection, or retention of consumers' personal information; and
  - any other practical and reliable method of calculation used in good faith.

Limitations on Compliance Obligations

- Among other exclusions, the CCPA does not apply to:
  - medical information governed by the Confidentiality of Medical Information Act, or protected health information governed by the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act;
  - information collected as a part of federally-regulated clinical trials;
  - personal information that is sold to or from a consumer reporting agency if it is used as part of a consumer report governed by the Fair Credit Reporting Act; or
  - personal information that is 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.
- To clarify, a consumer's right to sue a covered business for data breach under the CCPA would not be limited by the exclusions above. Such excluded information could still serve as a basis of a data breach lawsuit if the breached data happened to be non-encrypted or non-redacted personal information.
- A business may be able to avoid liability for any violation of the CCPA if the business trusts its contractually bound vendor with personal information and the vendor processing such information violates the CCPA. To avoid liability under this provision, the business must show that at the time of disclosing the personal information the business did not have actual knowledge, or reason to believe, that the vendor intended to violate the CCPA.
- The CCPA does not require a business to re-identify or otherwise link information that the business does not already maintain in a manner that would be considered personal information.
- Additionally, the CCPA clarifies its scope by stating that a business covered by the CCPA would not be restricted by the CCPA in the business's ability to:
  - comply with other laws, inquiries, investigations, and subpoenas, cooperate with law enforcement agencies, or exercise or defend legal claims;
  - collect, use, retain, sell, or disclose personal information that is de-identified or aggregated; or
  - collect or sell personal information collected during commercial conduct that takes place wholly outside of California.

Enforcement and Penalties

- A business that fails to cure a violation within 30 days will be fined by the California Attorney General for up to $2,500 for each uncured violation or up to $7,500 for each uncured intentional violation of the CCPA. The CCPA does not, however, define what constitutes a "violation."
- Under the CCPA, consumers have a private right of action against a business for data breaches if there is a violation of the business's obligations under the CCPA. To qualify as a data breach, there must have been an unauthorized access, exfiltration, theft, or disclosure of the consumer's unencrypted or non-redacted personal information due to the business's failure to implement and maintain reasonable security practices.
- Via this private right of action, a consumer may:
  - recover damages not less than $100 and not greater than $750 per consumer per incident, or actual damages, whichever is greater;
  - obtain injunctive or declaratory relief; or
  - obtain any other relief the court deems proper.

Companies should assess their existing privacy framework and determine whether any changes should be made to comply with the CCPA. The following identifies high-level steps companies should consider.

1

Confirm Whether and How the CCPA Applies to Your Company

Not all businesses that collect, process, or sell the personal information of California consumers will have to comply with the CCPA. Only those businesses that satisfy at least one of the law's three prongs in its definition of "business" will be required to comply. Notably, vendors that process personal information on behalf of a covered business may be liable for the vendor's violations of the CCPA if they are considered "service providers" to a covered business. If the CCPA appears to apply to your company, the next step is to determine whether any of the limitations on CCPA compliance listed above may apply to your company's activities.

2

Involve Stakeholders

Satisfying the CCPA's obligations may entail changes to a company's activities. For this reason, it is key for everyone in the company who is responsible for the handling of personal information, from executives to team leads, to be aware of the importance of achieving CCPA compliance. These stakeholders must understand that the CCPA is not a mere technical requirement; the legal risks for inadequate compliance could be significant.

3

Assess and Update Your Privacy and Cybersecurity Infrastructure

Before implementing a CCPA compliance program, you will want to ensure that key personnel are educated on both the CCPA and the company's handling of personal information. In particular, consider educating those in technical roles (e.g., software engineers and IT staff) and non-technical roles (e.g., HR managers, product leads, and marketers). Additionally, you may choose to assign, direct, or engage someone in a role focused on compliance or privacy oversight to help your company comply with the CCPA and, more generally, manage your customers' personal information.

Your employees also may have to handle new technical demands imposed by the law, such as the ability to promptly delete or disclose information in response to a consumer request. As a result, unless your existing privacy infrastructure is already robust enough to handle the addition of these new obligations, you should consider whether additional or reallocated resources are needed in advance of the CCPA's upcoming enforcement date and during subsequent ongoing compliance efforts.

4

Map and Inventory Data

Before you can determine what changes need to be made to your company's procedures for managing personal information, you need to know what kinds of personal information your company collects and what handling procedures currently apply. Once you gain a clear understanding of the kinds of personal information involved, you will be able to determine what CCPA requirements may apply to your company.

Mapping and inventorying means asking how personal information is collected, processed, stored, and shared. Consider asking yourself the following:

- What personal information is being collected?
- From what sources is your company collecting this personal information?
- For what business purpose is your company collecting the personal information?
- What level of consent has been sought from the consumer or user?
- Is your company collecting any data from children under 13 or between the ages of 13 and 16?

After assembling this knowledge about the universe of personal information that your company collects, you should investigate how that data is being processed and stored. Consider asking yourself:

- Where, how, and for how long is personal information being processed, stored, disclosed, or sold?
- How is the personal information protected (e.g., encrypted, anonymized, or pseudonymized) and who has access to it?
- To what third parties (including vendors) is the personal information disclosed, and under what circumstances?
- Is any sharing of personal information a "sale" under the CCPA?
    - If so, consider whether potential service provider and other exemptions apply.
- What internal records are kept of these processes?

5

Analyze Gaps and Set Priorities

Based on your newfound understanding of the data your company collects, you should review your company's practices for handling personal information as compared to those set forth in the CCPA. It will be helpful to identify any gaps between your company's practices and the

CCPA's requirements. After completing this gap analysis, you can set priorities for achieving CCPA compliance. These priorities will depend on the extent to which your company handles personal information of Californians and may be informed by other considerations, such as your budget and staffing resources. Use a list of priorities for planning which changes and updates should be handled first.

6

Implement Your Plan

Although it is important to make sure your highest priorities are kept at the top of the work list, at the same time, it may also be helpful to address some minor issues first to ensure your company is making steady progress. Your implementation plan should be periodically reviewed and updated to respond to technical issues and business developments that arise during implementation. Above all, your implementation plan should ensure that your company continues methodically on the path to compliance.

For example, your CCPA implementation plan might include the following elements:

- **Deciding whether and how to continue sharing activities that could be considered "selling" data.** Subject to certain exceptions, most sharing of information for any form of consideration will be considered "selling" such information, subject to the CCPA's opt-out obligations. Companies subject to the CCPA will need to determine whether their activities constitute "selling" under the CCPA and, if so, decide to approach their business practices differently or take steps to provide for an opt-out. One approach might be to include an opt-out link on every webpage that collects personal information. Your company should also consider whether it makes sense to offer financial incentives for consumers to permit the "selling" of their personal information.
- **Preserving data.** Responses to consumers' verifiable information requests cover a 12-month period preceding the business's receipt of a verifiable consumer request. Once the law takes effect in 2020, consumers will be able to request data for the preceding 12 months. As a result, your company should be aware that a request made in 2020 may require you to provide information relating to data collection practices in 2019 because of this 12-month "look back" at consumer information you handled in 2019. Therefore, as a best practice, you should preserve 2019 data on (i) the categories of personal information that were collected in the preceding 12 months, and (ii) the categories that were sold or disclosed for business purposes in the preceding 12 months. A CCPA data retention exception allows a business not to retain consumer's personal information it collected for a single, one-time transaction if such information is not normally sold or retained by the business.
- **Updating privacy documents.** The CCPA includes many new elements and consumer rights, along with specific language that must be included in both external- and internal-facing privacy notices. You should consider establishing parameters for updating these privacy notices and systematizing this process for smoother ongoing compliance.
- **Provide Notices of Collection**. Although employees are temporarily exempt from most of the CCPA's provisions until January 1, 2021, you must still provide them with a notice and continuously keep them informed of the categories of personal information collected

and the purposes for which your company uses these categories of personal information. Separately, before you collect the personal information of consumers, you must give them notice of what information you are about to collect, for what purpose, and how you plan to use it. Remember to continuously keep the consumers abreast of the types and methods of handling their personal information every time they happen to change.

- **Implementing a consumer request process.** Once the CCPA takes effect, California residents will be able to request information about the categories of personal information collected about them by businesses. Those businesses not already complying with other privacy regulations like the GDPR, which allows for similar data requests, will need to build a new process to accommodate such requests. It may be helpful for your company to templatize the process of responding to consumer requests in order to achieve consistency and scalability as you develop new consumer-facing products and grow your company. Consider forming a team dedicated to responding to consumer requests.
- **Managing vendors.** You should analyze which of your vendors are likely to be considered "service providers" under the CCPA. One useful practice may be for your contracts with service providers to include language barring the service provider from:
  - retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for your business;
  - using the personal information for purposes not otherwise permitted by the CCPA; and
  - retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with your business.
- Through such contracts, your company can ensure that service providers are complying with the data sharing and usage restrictions at the core of the CCPA and take advantage of the exemption from the law's definition of "selling" that exists for transfers of data to service providers.
- **Assessing security measures.** The CCPA grants a private right of action to consumers affected by a data breach, in addition to fines the California Attorney General may issue for such breaches. Your company must ensure that it is taking "reasonable" security measures to mitigate the risk of such breaches. Although this standard is not defined, in her **2016 Data Breach Report**, California's then-current Attorney General published a list of safeguards considered "reasonable." The report emphasized the 20 controls outlined by the Center for Internet Security, which can serve as useful guidance for compliance with this requirement.

7 Educate Employees and Customers

For the implementation plan to work, your company's employees must be involved in and supportive of the compliance process. This could include training and education on the basic principles of the CCPA and the compliance procedures being implemented by your company.

Though not required by the CCPA, you may consider educating your customers in the same way. The CCPA grants California consumers new rights about their personal information. Informing customers about those rights can help with fulfilling the CCPA's aim of transparency regarding personal information and, when customers exercise those rights, ensuring that they do so in a way that works with your company's internal processes. Consider incorporating this information into an updated privacy notice, a blog post or video, or sending it by email to customers.

8

Reassess Continually and Monitor Compliance

The compliance process will not necessarily be linear and will require periodic and frequent reviews and updates to ensure that your company is on track to comply with the CCPA. After attaining compliance, your company will need to maintain that status.

At least once every 12 months, the CCPA requires you to update your company's privacy policy with:

- a description of consumers' rights and the designated methods of submitting requests;
- a list of the categories of personal information that you have collected in the preceding 12 months;
- a list of the categories of personal information you have sold in the preceding 12 months; and
- a list of the categories of personal information you have disclosed about consumers for a business purpose in the preceding 12 months.

Consider updating your privacy policy to indicate that these requests are limited to a 12-month period from the date of the request in order to make sure you are able to comply with a verifiable consumer request by locating and providing the relevant personal information to the requesting consumer. After any update, state the date on which a given notice or privacy policy was last updated. Crucially, anytime your company intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, you must directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.

As a matter of good practice, and to prepare for greater ease of response to potential regulatory inquiries, keeping proper records is essential. Consider keeping records of consents obtained from California consumers, your company's data processing activities, and processes for protecting personal information. Consider whether it is practical and potentially beneficial from an operational perspective to integrate these records into your company's knowledge management system to facilitate continuous compliance.

Understanding the CCPA's requirements and implementing robust policies and procedures to comply with them are essential new tasks for businesses. Not only is the CCPA likely to become a major part of the regulatory landscape, lawmakers in numerous other states have recently introduced laws similar to the CCPA. Building a strong approach to data privacy in line with the CCPA's requirements will position your company for success when other laws at the state or federal level are enacted.

- [ ] Does the CCPA apply to my organization?
- [ ] Involve privacy and cybersecurity stakeholders
- [ ] Inventory the personal information you collect, access, or sell
- [ ] Assess whether data is being sold and whether exceptions might apply
- [ ] Analyze gaps and prioritize implementation milestones
- [ ] Create a process and develop tools for implementing consumer requests
- [ ] Provide updated privacy notice to consumers about their CCPA rights
- [ ] Update vendor agreements to include required CCPA language
- [ ] Educate consumers and train employees
- [ ] Continually monitor compliance

KEY CONTACTS

Lisa Monaco
Chair, Data Security and Privacy Practice
Washington, DC: +1 202 383 5413
New York: +1 212 326 2000
lmonaco@omm.com

Melody Drummond Hansen
Partner
Silicon Valley
+1 650 473 2636
mdrummondhansen@omm.com

Randall Edwards
Partner
San Francisco
+1 415 984 8716
redwards@omm.com

Daniel Suvor
Partner
Los Angeles
+1 213 430 7669
dsuvor@omm.com

Scott Pink
Special Counsel
Silicon Valley
+1 650 473 2629
spink@omm.com

ABOUT O'MELVENY

It's more than what you do: it's how you do it.

That's why O'Melveny is counsel of choice to an ever-expanding list of market leaders.

Across sectors and borders, from growth strategy to asset protection to navigating complex law and regulation, we measure our success by yours. And, in our interactions, we commit to making your experience of the firm as satisfying as the outcomes we help you achieve.

Our greatest achievement: ensuring that you never have to choose between legal and business excellence and inspired service

So, tell us. What do you want to achieve?

Century City • Los Angeles • Newport Beach • New York • San Francisco • Silicon Valley • Washington, DC
Beijing • Brussels • Hong Kong • London • Seoul • Shanghai • Singapore • Tokyo

omm.com