Weil

THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020

MAY 2021

The California Privacy Rights Act of 2020

On November 3, 2020, the California Privacy Rights Act of 2020 (CPRA) passed by a large margin as a ballot initiative in California. The CPRA broadly amends the California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, and has been enforceable by the office of the California Attorney General (AG) since July 1, 2020.

Most provisions of the CPRA will go into effect January 1, 2023 and be enforceable beginning July 1, 2023 but will apply to personal information collected by a covered business on or after January 1, 2022. As a result, businesses subject to the CPRA now have less than a year to address any necessary changes to their privacy policies and programs in order to be in compliance with the CPRA by January 1, 2022.

The new law tasks both the AG and a newly-formed state privacy agency, the California Privacy Protection Agency (CPPA), with adopting regulations further clarifying certain defined terms, exemptions and key obligations by July 1, 2022.

Because it is a ballot initiative, the CPRA cannot be amended through the legislative process in the way the CCPA was before it went into effect in January 2020. The CPRA will go into effect as drafted, with further ballot initiatives as the only avenue for amendment. The CPRA builds on the CCPA to align it much more closely with the EU's General Data Protection Regulation (GDPR).

The below includes: (I) an overview of the steps that businesses should take in the coming year to comply with the CPRA, followed by (II) a chart comparing the key aspects and requirements of the GDPR, CCPA and CPRA. Note that the GDPR includes numerous requirements that are not replicated in either the CCPA or CPRA and are therefore not accounted for in this memo, which is intended to compare CPRA requirements with similar requirements that appear in the GDPR or CCPA.

I. CPRA Compliance To-Do List

The following to-do list is a high-level overview of action items for businesses seeking to comply with the CPRA. Column 1 lists action items for businesses that are not subject to the GDPR and are already compliant with the CCPA. Column 2 lists action items for businesses that are already compliant with the GDPR and CCPA. Each listed item is addressed in greater detail in Part II.

1. CCPA-Compliant Businesses Not Subject to GDPR	2. GDPR- and CCPA-Compliant Businesses
Automated Decision-Making (new for California)	
Automated Decision-Making *For businesses that utilize automated decision-making.* ☐ Pending new regulations, disclose the logic involved in any automated decision-making technology as well as a description of the likely outcome of the process ☐ Expand opt-out function to include opt-out of the use of automated decision-making technology, including profiling	Automated Decision-Making *For businesses that utilize automated decision-making.* ☐ Likely already addressed per GDPR requirements, but businesses should review their disclosures to confirm compliance with CPRA regulations ☐ Expand opt-out function to include opt-out of the use of automated decision-making technology, including profiling
Data Minimization, Purpose Limitation & Storage Limitation (new for California)	
☐ Ensure that use, retention and sharing of personal information is "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed" or for another disclosed purpose	Policies and practices demonstrating adherence to these principles should already be in place per GDPR requirements
High-Risk Processing Activities (new for California)	
Subject to new regulations. ☐ Review practices with respect to data collection and use and identify processing that may present significant risk to consumers' privacy or security ☐ To the extent high-risk processing activities are identified, subject to implementing regulations, prepare a process for performing cybersecurity audits annually	*Subject to new regulations.* Same action items as Column 1, to the extent not already addressed by GDPR compliance efforts

1. CCPA-Compliant Businesses Not Subject to GDPR	2. GDPR- and CCPA-Compliant Businesses
Data Use Limitation & Opt-Out Functions and Processes	
<u>Sensitive Personal Information</u> ☐ Map data flows with respect to the collection, use and sharing of sensitive personal information ☐ Implement internal function to receive and respond to requests to limit the sharing of sensitive personal information ☐ Post "Limit the Use of My Sensitive Personal Information" link (or combine with "Do Not Sell My Personal Information" link)	<u>Sensitive Personal Information</u> Same action items as Column 1, to the extent not already addressed by GDPR compliance efforts
<u>Data Sharing</u> *For businesses that engage in cross-context behavioral advertising.* ☐ Expand opt-out function to include opt-out of data sharing ☐ Map practices and data flows with respect to the collection, use and sharing of personal information for the purpose of cross-context behavioral advertising, including data sources and parties to whom such information is disclosed	<u>Data Sharing</u> *For businesses that engage in cross-context behavioral advertising.* Same action items as Column 1
Updates to Privacy Policies & Notices	
<u>Website Privacy Policies</u> ☐ Add categories of sensitive personal information collected, purposes of collection and whether sold or shared ☐ Add new rights (request correction and restrict use and disclosure of sensitive personal information) ☐ If applicable, add disclosures regarding data sharing (i.e., cross-context behavioral advertising) ☐ Pending new regulations, add information about use of automated decision-making technology	<u>Website Privacy Policies</u> Same action items as Column 1, to the extent not already addressed by GDPR compliance efforts

(cont'd next page)

1. CCPA-Compliant Businesses Not Subject to GDPR	2. GDPR- and CCPA-Compliant Businesses
Updates to Privacy Policies & Notices (cont'd)	
<u>Notice at the Point of Collection</u> ☐ Add categories of sensitive personal information collected and purposes of such collection ☐ Add whether any personal information is sold or shared ☐ Add data retention periods for each category of personal information	<u>Notice at the Point of Collection</u> Same action items as Column 1, to the extent not already addressed by GDPR compliance efforts
Updates to Service Provider & Contractor Contracts	
<u>Identify Service Providers and Contractors</u> ☐ Review data disclosures to third parties to determine which third parties are service providers and which are contractors	<u>Identify Service Providers and Contractors</u> Same action item as Column 1
<u>Service Providers</u> *Update agreements already in compliance with CCPA requirements.* ☐ State that personal information is sold/disclosed for specified purposes ☐ Prohibit *sharing*, in addition to selling, personal information ☐ Prohibit retaining, using or disclosing personal information for any purpose other than as specified in the contract or outside of the direct business relationship between the parties (this prohibition should already appear in CCPA-compliant agreements) ☐ Prohibit combining personal information received from the business with personal information collected from service provider's interaction with consumer or from other sources ☐ Establish business's right to monitor service provider's compliance ☐ Require service provider to notify business (i) of any appointment of a subcontractor and bind subcontractors to the same terms to which the service provider is bound and (ii) if it determines it can no longer meet its CPRA obligations ☐ Require service provider to comply with the CPRA	<u>Service Providers</u> *Update agreements already in compliance with CCPA requirements.* Same action items as Column 1

(cont'd next page)

1. CCPA-Compliant Businesses Not Subject to GDPR	2. GDPR- and CCPA-Compliant Businesses
Updates to Service Provider & Contractor Contracts (cont'd)	
☐ Provide business the right to (i) ensure service provider uses personal information consistent with business's CPRA obligations and (ii) stop and remediate any unauthorized use of personal information ☐ Require service provider to provide assistance to business in connection with responding to consumer requests and fulfilling certain of the business's CCPA obligations	
<u>Contractors</u> *Enter into agreements or update existing agreements.* ☐ State that personal information is sold/disclosed for specified purposes ☐ Prohibit selling or sharing personal information ☐ Prohibit retaining, using or disclosing personal information for any purpose other than as specified in the contract or outside of the direct business relationship between the parties ☐ Prohibit combining personal information received from the business with personal information collected from contractor's interaction with consumer or from other sources ☐ Require certification that contractor understands and will comply with all specified restrictions ☐ Establish business's right to monitor contractor's compliance ☐ Require contractor to notify business (i) of any appointment of a subcontractor and bind subcontractors to the same terms to which the contractor is bound and (ii) if it determines it can no longer meet its CPRA obligations ☐ Require contractor to comply with the CPRA ☐ Provide business the right to (i) ensure contractor uses personal information consistent with business's CPRA obligations and (ii) stop and remediate any unauthorized use of personal information ☐ Require contractor to provide assistance to business in connection with responding to consumer requests and fulfilling certain of the business's CCPA obligations	<u>Contractors</u> *Enter into agreements or update existing agreements.* Same action items as Column 1

(cont'd next page)

1. CCPA-Compliant Businesses Not Subject to GDPR	2. GDPR- and CCPA-Compliant Businesses
Updates to Service Provider & Contractor Contracts (cont'd)	
Third Parties *Enter into agreements or update existing agreements.* ☐ State that personal information is sold/disclosed for specified purposes ☐ Require third party to notify business if it determines it can no longer meet its CPRA obligations ☐ Require third party to comply with the CPRA ☐ Provide business the right to (i) ensure third party uses personal information consistent with the business's CPRA obligations and (ii) stop and remediate any unauthorized use of personal information	Third Parties *Enter into agreements or update existing agreements.* Same action items as Column 1

II. Comparison Chart

The following chart is a non-exhaustive, high-level overview of key provisions of the CPRA and applicable parallels in the GDPR and/or CCPA.

Components	GDPR	CCPA	CPRA
Applicability	Any entity processing personal data that is (i) established in the EU or (ii) not established in the EU but processes EU residents' personal data in connection with offering goods or services in the EU or monitoring EU residents' behavior.	For-profit entities in any jurisdiction that (i) do business in CA and control the means of processing personal information; and (ii) one of: (a) over $25 million in annual gross revenues; (b) purchase, sale, or sharing of personal information of 50,000 or more consumers, households or devices annually; or (c) more than half of annual revenues derived from selling consumer personal information.	For-profit entities in any jurisdiction that (i) do business in CA and control the means of processing personal information; and (ii) one of (a) over $25 million in annual gross revenues; (b) purchase, sale, or sharing of personal information of 100,000 or more consumers or households ~~or devices~~ annually; or (c) more than half of annual revenues derived from selling or sharing consumer personal information.
Key Defined Terms	■ "Controller" is a natural or legal person, public authority, agency or other body that, alone or jointly, determines the purposes and means of processing personal data. ■ "Processor" is a natural or legal person, public authority, agency or other body that processes personal data on behalf of a controller. ■ "Processing" is any operation performed on personal data, including collection, recording, organizing, storing, altering, disclosing, etc.	■ "Business" is an entity subject to the CCPA. ■ "Service Provider" is an entity that processes information on behalf of a business and to which a business discloses a consumer's personal information for a business purpose pursuant to a written contract. ■ "Sell" means any disclosure of personal information by a business to another business or third party for money or other valuable consideration, subject to certain exceptions.[1]	■ "Business" is an entity subject to the CPRA. ■ "Service Provider" is a~~n entity~~ person that processes personal information on behalf of a business and receives from or on behalf of the business a consumer's personal information pursuant to a written contract. ■ "Contractor" is a person to whom a business provides a consumer's personal information for a business purpose pursuant to a written contract. ■ "Sell" means any disclosures of personal information by a business to ~~a another business or~~ third party for money or other valuable consideration, subject to certain exceptions.

[1] Notable exceptions include when (i) a consumer directs the business to disclose personal information to a third party, provided that third party does not sell the information, (ii) the business shares personal information with a service provider, and (iii) personal information is transferred as part of a business transaction.

Components	GDPR	CCPA	CPRA
			■ "Share" means to make available personal information to a third party for cross-context behavioral advertising (e.g., advertising across different, non-affiliated websites).
Required Public Policies and/or Notices[2]	■ Where personal data is collected directly from a data subject, notice must be provided at the time of collection. ■ Where personal data is obtained indirectly, the controller must provide the data subject with notice within a reasonable period (i) after obtaining the personal data (at the latest within one month), (ii) before or when first communicating with the data subject (if applicable) or (iii) before or when disclosing the personal data to another recipient (if applicable).	■ Businesses must provide two or more methods for submitting requests for information, including a toll-free telephone number. ■ Businesses must make disclosures of their privacy practices on their websites. ■ Businesses must provide notice at or before the point of collection of personal information. ■ Per CCPA regulations, businesses must provide a "just in time" pop-up notice where personal information is collected on a mobile device in a manner that a consumer would not reasonably expect.	■ Businesses must provide two or more methods for submitting requests for information, including a toll-free telephone number. ■ Businesses must make disclosures of their privacy practices on their websites. ■ Businesses must provide notice at or before the point of collection of personal information. ■ It is not yet clear if the "just in time" notice will be retained under the CPRA once new regulations are in place.
Protected Data	Personal Data means any information relating to an identified or identifiable natural person ("data subject").	Personal Information includes any information that is reasonably capable of being associated with a particular consumer or household.	Same definition of Personal Information.
Sensitive Data	■ Sensitive personal data includes: □ background and beliefs (i.e., racial or ethnic origin, political or religious opinions, union membership, sexual orientation, etc.); □ genetic data or biometric data processed to identify an individual;	N/A	■ Sensitive personal information includes: □ government-issued IDs (i.e., social security, driver's license, passport); □ financial account information (i.e., credit card, bank account, login credentials); □ precise geolocation data;

[2] See Appendix A for an outline of required disclosures to be made in each type of privacy policy/notice.

Components	GDPR	CCPA	CPRA
	☐ health-related data. ■ Processing such data is permitted only under enumerated circumstances, including where a data subject gives explicit consent.		☐ background and beliefs (i.e., racial or ethnic origin, religious beliefs, union membership, sexual orientation); ☐ contents of mail, email and text messages; ☐ genetic data and biometric information; ☐ health-related information. ■ Consumers have the right to direct businesses that collect sensitive personal information to limit use of such information to that which is necessary to perform services or provide goods reasonably expected.
Exempted Data	■ Personal data processed in connection with purely personal or household activities. ■ Personal data processed by governmental authorities for law enforcement purposes. ■ Personal data processed pursuant to safeguarding national security. ■ Personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable.	■ Personal information of employees and job applicants is largely exempted from the CCPA's requirements through the end of 2021 (but employers must provide employees with a compliant privacy notice, and employees may utilize the private right of action associated with certain data breaches). ■ Personal information collected in the context of communications between two businesses is exempted from several requirements (but is subject to the right to opt-out of the sale of personal information and the private right of action associated with certain data breaches). ■ Data covered by certain other privacy laws is exempted (i.e., health information that would be covered by other laws governing health/ medical data).	■ Both CCPA exemptions are extended through the end of 2022. ■ Same exemption regarding data covered by certain other privacy laws. ■ Same exclusion regarding deidentified or aggregated consumer information.

Components	GDPR	CCPA	CPRA
		■ Deidentified or aggregated consumer information.	
Right to Access or Know	■ Controllers must have a process to receive and respond to data subject requests for: □ confirmation as to whether their personal data are being processed; □ access to such personal data; and □ information concerning the purposes of processing, categories of personal data processed, any third parties to whom personal data has or will be disclosed, retention period for such data, source(s) of the data and details regarding any automated decision-making. ■ Controllers must provide individuals with notice of their rights, including the right to request rectification, erasure or restriction of the processing of the data and the right to lodge a complaint with a supervisory authority. ■ Controllers must provide individuals access to information concerning the safeguards used in connection with any international transfer of personal data.	■ Businesses must have a process to receive and respond to "verified" consumer requests for details regarding the personal information about the requesting consumer that the business processes. ■ Businesses must provide, for the preceding 12-month period: □ the categories and specific pieces of personal information the business has collected from or about the consumer; □ the categories of personal information that the business has shared or sold, if any; □ the business or commercial purposes for collecting or selling personal information; □ the categories of sources from which the personal information was collected; and □ per category of personal information shared or sold, the categories of third parties with whom personal information is so shared or sold.	■ Same requirements regarding "verified" consumer requests. ■ Same requirements regarding the categories of information to be provided. ■ In addition, a business must disclose categories of information it has collected about a consumer both directly and indirectly, including through or by a service provider or contractor. ■ Pending new regulations, consumers may request that a business disclose information beyond the preceding 12-month period in connection with personal information collected on or after Jan. 1, 2022. ■ Pending new regulations, consumers have a right to receive meaningful information about the logic involved in any automated decision-making technology as well as a description of the likely outcome of the process.
Right to Delete	■ Controllers must respond to requests from data subjects for erasure of their personal data.	■ Businesses must have a process in place to receive and respond to "verified" consumer requests to delete their personal information.	■ Same requirements regarding process to receive and respond to "verified" consumer requests.

Components	GDPR	CCPA	CPRA
	■ Exceptions include where processing is necessary (a) to exercise freedom of expression rights; (b) to comply with a legal obligation imposed by EU or member state law; (c) for reasons of public health interest; (d) for archival purposes in the public interest, scientific or historical research purposes or statistical purposes or (e) for the establishment, exercise or defense of legal claims. ■ Where obligated to delete personal data, controllers must take reasonable steps to inform other controllers, processors and anyone else to whom the controller disclosed the data of the individual's request.	■ Upon verifying a request, the business must delete the consumer's personal information and direct service providers to delete information held on the business's behalf. ■ Exceptions include where retention is necessary for: (a) performance of the contract between the business and the consumer; (b) detecting and addressing security incidents; (c) identifying and repairing bugs; (d) exercising free speech or other rights under the law; (e) complying with criminal proceeding requirements; (f) enabling internal uses "reasonably aligned" with consumer expectations; or (g) otherwise internally using the consumer's personal information in a lawful manner that is compatible with the context in which the consumer provided the information.	■ Same requirements regarding deletion and direction to service providers. ■ Service providers and contractors must cooperate with the business in responding to a request for deletion, including notifying their own service providers and contractors. ■ Largely the same exceptions apply as under the CCPA.
Right to Correct	Data subjects have a right to rectify inaccurate personal data regarding them, including to have incomplete personal data completed.	N/A	■ Consumers have a right to request that a business correct inaccurate personal information maintained about them. ■ Businesses that receive a verifiable consumer request for correction must use "commercially reasonable efforts" to correct such information.

Components	GDPR	CCPA	CPRA
Right to Restrict, Object, or Opt-Out of Sale or Sharing	Data subjects have the right to: ■ restrict processing under certain circumstances, such as where the accuracy of the personal data is contested or the processing is unlawful but the data subject requests restriction instead of erasure; ■ object at any time to processing of their personal data, where the basis of processing is "public interest" or "legitimate interest."	■ Consumers have the right to direct a business that sells personal information to third parties not to sell their personal information. ■ Businesses that sell personal information must provide notice to consumers that such information may be sold and that consumers have a right to opt-out. ■ Businesses that sell personal information must have a "clear and conspicuous" link on their website that reads "Do Not Sell My Personal Information." Clicking the link must take users to a webform enabling opt-out.	■ Consumers have the right to direct a business that sells or shares personal information to third parties not to sell or share their personal information. ■ Businesses that sell or share personal information must provide notice to consumers that such information may be sold or shared and that consumers have a right to opt-out. ■ Pending new regulations, consumers may opt-out of a business's use of automated decision-making technology, including profiling. ■ If a business shares personal information, the link required by the CCPA must be updated to read "Do Not Sell or Share My Personal Information." ■ Businesses must provide a link titled "Limit the Use of My Sensitive Personal Information" that enables consumers to restrict the use of sensitive personal information. ■ Businesses may use one single "clearly-labeled" link to comply with both above requirements. ■ Pending new regulations, businesses may be able to elect not to use such links if they offer technology that enables consumers to send an "opt-out preference signal."
Right to Data Portability	Data subjects have the right to receive their personal data in a structured, commonly used and machine-readable format.	Consumers have the right to receive requested information in a format that is easily understandable, machine-readable and able to be easily transmitted to another entity.	Same rights as under the CCPA.

Components	GDPR	CCPA	CPRA
Responding to Requests	Controllers must provide the data subject with information on action taken on a request (or reasons for not taking action) within one month of receipt, which may be extended by two months where necessary.	Businesses must: (a) confirm receipt within 10 business days and respond to any verified request within 45 calendar days (with limited exceptions); (b) verify a requesting consumer's identity; and (c) maintain records of consumer requests for at least 24 months, including the manner of response.	Same requirements regarding the timing of confirmation of receipt and response.
Non-Discrimination Requirements	Data subjects have the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects or similarly significantly affects the data subject.	Businesses may not discriminate against consumers who exercise their rights by denying products or services, charging or suggesting different prices or offering different levels or quality of goods or services.	Businesses may not discriminate against consumers, employees, job applicants or independent contractors for exercising their rights under the law.
Purpose Limitation Requirements	Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.	N/A	Collection, use, retention and sharing of personal information must be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed or for another disclosed purpose.
Data Retention Restrictions	Personal data must be kept for no longer than necessary for the purposes for which it is processed.	N/A	Businesses may not retain personal information for longer than is reasonably necessary for each disclosed purpose for which the information was collected.
Data Security Requirements Security	Both controllers and processors must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk associated with the processing.	Businesses have an implicit duty to implement and maintain reasonable security procedures and practices to protect personal information, which must be appropriate to the nature of such information.	Businesses, service providers and contractors have an explicit duty to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification or disclosure.

Components	GDPR	CCPA	CPRA
Risk Assessment Requirements	■ When processing is likely to result in a high risk to the rights and freedoms of data subjects, controllers must conduct a data protection impact assessment ("DPIA") to assess the impact such processing will have on the protection of personal data, including a threshold assessment of whether the "high risk" threshold is met.	N/A	Businesses whose processing of personal information presents "significant risk" (subject to new regulations) to consumers' privacy or security must: ■ perform an annual independent cybersecurity audit; ■ submit a risk assessment to the CPPA on a regular basis, including whether the business processes sensitive personal information and weighing the benefits from the processing against the risks to consumers' privacy.
Training Requirements	The GDPR does not explicitly require training, although the enumerated responsibilities of the data protection officer include training of relevant staff. Controllers must also implement appropriate measures to ensure GDPR compliance, which for many controllers would likely include training.	Businesses must train all individuals responsible for handling consumer inquiries about the business's privacy practices and compliance regarding all relevant requirements and how to direct consumers to exercise their rights.	Same requirements as under the CCPA.
Protections for Minors	Where an entity processes personal data of a child under 16 in the context of offering services to the child and based on consent, that processing is only lawful if consent is given by the child's parent or guardian.	Businesses may not sell personal information of a consumer the business knows to be under 16, unless (i) the guardian of a consumer under 13 affirmatively consents or (ii) the consumer is between the ages of 13 and 16 and affirmatively consents.	Businesses may not sell or share personal information of a consumer the business knows to be under 16, unless (i) the guardian of a consumer under 13 affirmatively consents or (ii) the consumer is between the ages of 13 and 16 and affirmatively consents.

Components	GDPR	CCPA	CPRA
Required Agreements	Processing on behalf of a controller must be governed by a contract that is binding on the processor and includes information on the processing and various required provisions relating to, among other things, the implementation of appropriate security measures, the use of subprocessors and assistance with the controller's compliance obligations (e.g., the fulfillment of data subject requests and demonstrating compliance with the GDPR).	■ No required agreements. ■ To ensure a third party meets the definition of a service provider (and thus reduce the likelihood that personal information shared with that third party will be categorized as a "sale"), a business must enter into an agreement limiting the service provider's use of personal information, prohibiting the sale of such information, and requiring the service provider to certify it understands and intends to comply with its obligations.	■ Agreements are required with (i) third parties to or with whom personal information is sold or shared and (ii) service providers and contractors to whom personal information is disclosed. ■ Contract requirements vary based on whether the entity processing data on behalf of or provided by the business is a service provider, contractor or third party (see Part I).
Private Right of Action	Any person who has suffered damage as a result of a violation of the GDPR has the right to receive damages from the responsible controller or processor by bringing an action in the courts of the applicable EU member state.	A consumer whose nonencrypted or nonredacted personal information is subject to a breach as a result of a business's violation of its obligation to maintain reasonable security practices may bring a civil action.	A consumer whose nonencrypted and nonredacted personal information, or email address in combination with information permitting access to the account, is subject to a breach as a result of a business's violation of its obligation to maintain reasonable security practices may bring a civil action.
Enforcement	■ Each EU member state has a supervisory authority tasked with enforcing the GDPR. ■ Supervisory authorities may impose administrative fines, subject to consideration of a number of factors, but ultimately up to the higher of 20 million euros or 4% of total worldwide annual turnover. ■ The GDPR does not explicitly provide for criminal liability, but it does allow for member states to implement "other penalties," including criminal penalties.	■ The AG has primary enforcement responsibility. ■ The AG may seek both injunctive and monetary penalties, up to $2,500 per violation or $7,500 per intentional violation. ■ Businesses are to be provided notice of a violation and a 30-day period to cure before the AG may issue any penalty.	■ Both the AG and the newly-created CPPA have enforcement responsibility. ■ The CPPA may investigate possible violations on its own initiative or on receipt of a sworn complaint, hold administrative hearings and issue cease-and-desist orders and fines up to $2,500 per violation or $7,500 per intentional violation or violation involving personal information of consumers under 16 years of age. ■ The AG may request a stay of a CPPA administrative action in order to be able to proceed with an investigation or civil action. ■ The CPRA provides no cure period, but the CPPA has discretion to offer a cure period.

Appendix A
Privacy Policies & Notices

GDPR

- Notice At Collection From Data Subject. Controllers that collect personal data *from the data subject* must provide the data subject with the following information at the time of collection:
    - the identity and contact details of the controller and, where applicable, the controller's EU representative;
    - the contact details of the data protection officer, where applicable;
    - the purposes and legal basis for the processing (including the legitimate interests pursued, if applicable);
    - the recipients or categories of recipients of the personal data, if any;
    - where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the EU Commission, or reference to the appropriate safeguards and how to obtain a copy;
    - the retention period for the personal data, or if that is not possible, the criteria used to determine that period;
    - the existence of the right to request access, rectification, erasure or restriction of processing with respect to the personal data, to object to the processing, or to request a portable copy of the personal data;
    - the existence of the right to withdraw consent, where the processing is based on consent;
    - the right to lodge a complaint with a supervisory authority;
    - whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obligated to provide the personal data and of the possible consequences of failure to provide such data; and
    - the existence of automated decision-making, plus meaningful information about the logic involved and the significance and the envisaged consequences of such processing for the data subject.
- Notice At Collection From Other Sources. Controllers that obtain personal data *from a source other than the data subject* must provide the data subject with the following information:
    - the identity and contact details of the controller and, where applicable, the controller's EU representative;
    - the contact details of the data protection officer, where applicable;
    - the purposes and legal basis for the processing (and where based on legitimate interests, the interests pursued);
    - the categories of personal data concerned;
    - the recipients or categories of recipients of the personal data, if any;
    - where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the EU Commission,

or reference to the appropriate safeguards and how to obtain a copy;

- the retention period for the personal data, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- the existence of the right to withdraw consent, where the processing is based on consent;
- the right to lodge a complaint with a supervisory authority;
- from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; and
- the existence of automated decision-making, plus meaningful information about the logic involved and the significance and the envisaged consequences of such processing for the data subject.

In addition:

- Notices must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child under 16;
- Notices must be provided in writing, or by other means, including, where appropriate, by electronic means; and
- When requested by the data subject, notices may be provided orally, provided the identity of the data subject is proven by other means.

CCPA/CPRA

- Privacy Policy. The CCPA requires covered businesses to provide a publicly-available privacy policy that includes the following specific disclosures (to be updated annually):
  - a description of consumers' rights under the CCPA/CPRA, including instructions for submitting requests, the process used to verify requests, and instructions on how an authorized agent can make a request;
  - for the preceding 12 months, separate lists of each of:
    - the categories of personal information collected about consumers by the business,
    - the categories of personal information disclosed about consumers for a business purpose (or a statement that no such information has been disclosed), and
    - the categories of personal information sold to or shared with a third party (or a prominent statement that the business has not sold or shared personal information);
  - the categories of sources from which the personal information is collected;
  - the business or commercial purpose for collecting or selling or sharing personal information;
  - the categories of third parties to whom the business discloses consumers' personal information;
  - a statement as to whether the business has actual knowledge that it sells the personal information of minors under 16 and, if so, a description of the process for obtaining required opt-in consent from a parent or guardian (minors under 13) or from the minor directly (minors 13–16);
  - a prominent statement that the business does not sell personal information or, for businesses that do

sell personal information within the meaning of the CCPA, a "clear and conspicuous link" titled "Do Not Sell or Share My Personal Information" to an opt-out form;

- a "clear and conspicuous link" titled "Limit the Use of My Sensitive Personal Information" to a form enabling a consumer to limit the use or disclosure of that consumer's sensitive personal information (where applicable, this link may be combined with the "Do Not Sell or Share My Personal Information" link);
- two contact methods (one of which must be a toll-free telephone number); and
- the date the privacy policy was last updated.

In addition:

- privacy policies must be available in the same languages in which the business enters into contracts and makes other information available to consumers;
- covered businesses must ensure that privacy policies are reasonably accessible to consumers with disabilities; and
- businesses that buy/receive and/or sell the personal information of 10,000,000 or more consumers in a calendar year must make certain additional disclosures, including metrics on the number of requests received and whether they were complied with.

- Notice At Collection. Covered businesses *that ~~collect~~ control the collection of personal information from consumers* must provide disclosures "at or before the point of collection" of personal information that include:
  - the categories of personal information to be collected and whether such information is sold or shared;
  - the business or commercial purpose for which that personal information will be used;
  - if the business collects sensitive personal information, the categories of such information to be collected, the purposes of such collection and use, and whether such information is sold or shared;
  - the length of time each category of personal information and sensitive personal information will be retained;
  - if the business sells personal information, the link titled "Do Not Sell My Personal Information" (required by the CCPA regulations, but will likely need to be updated to include applicable Do Not Share and Limit the Use of My Sensitive Personal Information language); and
  - for all individuals other than employees (per the regulations), a link to the business's privacy policy.

  The CCPA regulations clarify that for data collected online, a business may provide a link to the relevant section of its privacy policy in lieu of providing a separate notice.
- Just-In-Time Notice. Under the CCPA, the regulations require businesses that collect personal information from mobile devices "for a purpose that the consumer would not reasonably expect" to provide a "just-in-time" notice (e.g., a pop-up notice on the device) summarizing the categories of personal information being collected through the device and providing a link to the business's full notice at collection. It is not clear whether this will remain the case once the CPRA goes into effect and new regulations are adopted.
- Notice of Right to Opt-Out and of Financial Incentive. The CCPA includes as separate requirements that covered businesses must provide a notice of the right to opt-out of the sale of personal information and a notice of any financial incentives provided in connection with the sale of personal information. In practice, such notices are likely to be provided within a business's privacy policy and/or notice at collection but may be addressed through separate notices.