California Consumer Privacy Act Summary

On June 28, 2018, Governor Jerry Brown (D) signed the "California Consumer Privacy Act" (CCPA) into law. In November of 2020, California voters approved Proposition 24, the "California Privacy Rights Act", to amend and extend the CCPA. The original CCPA became effective on January 1, 2020. While the CPRA became effective January 1, 2023, enforcement of the first set of implementing regulations finalized by the California Privacy Protection Agency (CPPA) were delayed until March 29, 2024 . Please note that another set of draft regulations is expected to be released later in 2023 on the topics of risk assessment and cybersecurity audit. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **California Consumer Privacy Act (CCPA)** applies for-profit businesses that do business in California and meet any of the following criteria: (a) as of January 1 of the calendar year, had annual gross revenues of at least $25 million in the preceding calendar year; (b) alone or in combination, annually buys, sells, or shares the personal information of at least 100,000 consumers or households or devices; or (c) derives at least 50% of their annual revenue from selling or sharing consumers' personal information.
Covered Data	***"Personal Information"***: information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. ***"Sensitive Personal Information"***: Personal information that reveals: (a) a consumer's social social security, driver's license, state identification card, or passport number; (b) a consumer's account log-in, financial account, debit card, or credit card in combination with any required security or access code, password, or credentials allowing access to an account; (c) a consumer's precise geolocation; (d) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; (e) the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; (f) a consumer's genetic data. The term also applies to: (a) the processing of biometric information for the purpose of uniquely identifying a consumer; (b) personal information collected and analyzed concerning a consumer's health; (c) personal information collected and analyzed concerning a consumer's sex life or sexual orientation.
Key Definitions	***"Consent"***: any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person activating as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined purpose. ***"Dark Pattern":*** a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice. ***" De-Identified Data"***: information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information: (a) takes reasonable measures to ensure that the information cannot be associated with a consumer or household; (b) publicly commits to maintain and use the information in de-identified form and not to attempt to re-identify the information, except for the sole purpose of determining whether the business' de-identification processes satisfy the Act's requirements; and (c) contractually obligates any recipients of the information to comply with all provisions. ***"Pseudonymous Data"***: the processing of personal information in a manner that render the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and

	organizational measures to ensure that the personal information is not attributed to an identified or identifiable customer. ***"Cross-context behavioral advertising"***: the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts. ***"Sell", "selling", "sale", or "sold":*** 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 a third party for monetary or other valuable consideration.
Consumer Rights	• **Access:** A consumer has the right to request that a business that collects personal information about the consumer disclose the following: (a) the categories of personal information it has collected about that consumer; (b) the categories of sources from which the personal information is collected; (c) the business or commercial purpose for collecting, selling, or sharing personal information; (d) the categories of third parties to whom the business discloses personal information; (e) the specific pieces of personal information it has collected about the consumer. • **Affirmative Consent:** A business shall not sell or share the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowing of the consumer's age. • **Correction:** A consumer has the right to request a business that maintains inaccurate personal information about the consumer to correct the inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information. • **Deletion**: A consumer has the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. • **Limit:** A consumer has the right to limit use of personal information. A consumer may direct businesses to only sensitive personal information for limited purposes, such as providing requested services. • **Portability:** A consumer has the right to receive required information disclosures in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. • **Opt Out Rights**: A consumer has the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information.
Business Obligations	• **Responding to Consumer Requests**: A business shall, in a form that is reasonably accessible to consumers: (a) make available to consumers two or more designated methods for submitting requests for information required to be disclosed or requests for deletion or correction, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed or for requests for deletion or correction; (b) disclose and deliver the required information to a consumer free of charge, correct inaccurate personal information, or delete a consumer's personal information,

	based on the consumer's request, within 45 days of receiving a verifiable consumer request. The time period to comply with the consumer request may be extended once by an additional 45 days when reasonably necessary, taking into account the complexity and number of requests, provided the consumer is provided notice of the extension within the initial 45-day period along with the reason(s) for the delay. If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and within the permitted response time period, along with the reasons for not taking action and any rights the consumer may have to appeal the decision to the business. If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verifiable consumer request is manifestly unfounded or excessive. • **Data Minimization**: A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice. • **Avoid Secondary Use**: A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice. • **Data Security**: A business that collects a consumer's personal information shall 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. • **No Unlawful Discrimination:** A controller shall not discriminate against a consumer for exercising any consumer rights. • **Transparency**: A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of the following: (a) the categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared; (b) if the business collects sensitive personal information the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared; (c) the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine the period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose. • **Purpose Specification:** A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

Data Protection Assessments	Note that this is not currently a requirement. However, the California Privacy Protection Agency Board will issue related regulations as part of its cybersecurity rules to require businesses who process personal information that presents a significant risk to consumers' privacy or security to perform an annual cybersecurity audit.
Exceptions and Exemptions	• CCPA shall not be construed to restrict a controller's or processor's ability to: (a) comply with laws; (b) comply with inquiries by government authorities; (c) cooperate with law enforcement agencies concerning conduct that the business, service provider, or third party reasonably and in good faith believes may violate, federal, state, or local laws; (d) cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury under certain circumstances; (e) exercise or defend legal claims; (f) collect, use, retain, sell, share, or disclose consumers' personal information that is de-identified or aggregate or consumer information; (g) collect, sell, or share a consumer's personal information if every aspect of that commercial conduct take place wholly outside of California. • Data exempt from CCPA includes: protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, the Gramm-Leach-Bliley Act, vessel information or ownership information retained or shared between a vessel dealer and the vessel's manufacturer as defined in the Harbors and Navigation Code, and nonprofits.
Enforcement	• The CCPA established a new government agency, the California Privacy Protection Agency (CPPA) which is vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. Any business, service provider, contractor, or other person that violates the CPPA shall be liable for an administrative fine not to exceed $2,500 for each violation or $7,500 for each intentional violation or violations involving the personal information of consumers whom the business, service provider, contractor, or other person has actual knowledge are under 16 years of age in an administrative enforcement action brought by the CPPA. • The CCPA establishes a **limited private right of action**. Any consumer whose non-encrypted and non-redacted personal information, or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil act to recover damages, for injunctive or declaratory relief, or any other relief the court deems proper. • **Right to Cure**: The CPRA eliminated the CCPA's original mandatory 30-day cure period; instead, **the amended CCPA grants both the attorney general and the CPPA discretion on whether to offer a cure period**, taking into consideration a business' lack of intent to violate the CCPA and any voluntary efforts to cure the alleged violation. Under the **limited private right of action**, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer must provide a business 30 days' written notice identifying the specific provisions the consumer alleges have been or are being violated. If within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. The implementation and maintenance of reasonable security procedures and practices following a breach does not constitute a cure with respect to that breach. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations.