

CALIFORNIA PRIVACY RIGHTS ACT OF 2020: SUMMARY OF NEW RIGHTS & OBLIGATIONS

- **Purpose Limitation & Data Minimization:** Businesses must limit their collection, use, retention, and disclosure of personal information to that which is “reasonably necessary” and “proportionate” to achieve its intended purpose.
- **New Right to Correction:** Businesses must provide consumers with the ability to correct inaccurate personal information.
- **New Obligations Related to “Sharing”:** Businesses that “share” personal information are required to provide consumers with notice of this practice and the ability to opt out. “Sharing” is defined as transferring or otherwise communicating a consumer’s personal information to a third party for cross-context behavioral advertising (a concept that is similar to targeted advertising or interest-based advertising).
- **New Obligations Related to Sensitive Personal Information:** Businesses that collect “sensitive personal information” must disclose how they collect, use, and disclose this information and provide consumers with the ability to limit the use and disclosure of this information. “Sensitive personal information” includes, but is not limited to, account log-in credentials, precise geolocation information, biometric information, genetic and health data, social security number or other government-issued identification card number, and information related to race, ethnicity, religion, or sexual orientation.
- **Broader Timeframe for Access Right:** Businesses must provide information to consumers beyond the CCPA-mandated 12-month period preceding the request, unless doing so would be impossible or involve a disproportionate effort.
- **New Disclosure Requirements:** Businesses must disclose the length of time they retain each category of personal information collected or the criteria that will be used to determine such period. Businesses must also disclose the new consumer rights afforded under the CPRA, including the right to correction, the right to opt out of sharing, and the right to limit the use and disclosure of sensitive personal information.
- **Changes to Deletion Requirements:** Businesses that receive verifiable consumer requests to delete personal information must notify service providers and contractors to delete the personal information from their records. Businesses must also notify third parties to whom they have sold or shared such personal information to delete the personal information, unless doing so would prove impossible or involve disproportionate effort.
- **Downstream Contractual Restrictions:** Businesses must impose specific contractual obligations on service providers, contractors, and third parties before selling, sharing or disclosing personal information to them.
- **New Security Requirements and Expanded Data Breach Liability:** Businesses must implement reasonable security procedures and practices appropriate to the nature of the personal information they collect and maintain. The CPRA also expands the private right of action to apply to data breaches that compromise a consumer’s email address in combination with a password or security question and answer that would permit access to the consumer’s account.
- **B2B and Employee Personal Information:** While B2B and employee personal information have largely been exempted from the CCPA, the CPRA extends consumer rights and protections to this information.
- **Additional Obligations to be Developed in Rulemaking:** Businesses will have additional obligations once the CPRA regulations are issued. The newly-created California Privacy Protection Agency will have primary rulemaking authority, and final CPRA regulations will be adopted by July 1, 2022. Regulations are expected to cover 22 different areas, including the use of automated decision-making technology (including profiling), risk assessments, and recordkeeping.