Computer & Communications
Industry Association
Tech Advocacy Since 1972

'Colorado Privacy Act' Summary

On July 7, 2021 Governor Polis signed SB21-190, the "Colorado Privacy Act" ('CPA') into law. The majority of the Act's provisions take effect on July 1, 2023. A non-comprehensive summary of significant elements of the CPA follows:

Covered Entities	● The CPA applies to controllers that conduct business in, or produce/deliver products or services **intentionally targeted** to Colorado residents that (1) annually control or process the personal information of 100,000+ consumers, **and/or** (2) derive revenue or receive a discount on the price of goods or services from the sale of personal data and process or control the personal data of 25,000+ consumers.
Covered Data	● "**Personal data"** means information that is linked or reasonably linkable to an identified or identifiable individual and does not include de-identified data or **publicly available information** (information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public). ● **"Sensitive data"** means (a) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status; (b) genetic or biometric information that may be processed for the purpose of uniquely identifying an individual; (c) personal data from a known child.
Key Definitions	● ***"Sale"***: the exchange of personal data for monetary or other valuable consideration by a controller to a third party. The term includes multiple carve outs including disclosures to a processor that processes the data on behalf of a controller; disclosures for the purpose of providing a product or service requested by the consumer; disclosure to an affiliate of the controller; disclosure or transfer to a third party as part of a proposed or actual merger, acquisition, or bankruptcy; and disclosures that a consumer directs or intentionally makes available by a channel of mass media. ● ***"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"***: data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses the data: (a) takes reasonable measures to ensure that the data cannot be associated with an individual, (b) publicly commits to maintain and use the data only in a de-identified fashion without attempting to re-identify the data, and (c) contractually obligates any recipients of the information to comply with these requirements. ● ***"Pseudonymous Data"***: personal data that can no longer be attributed to a specific individual without the use of additional information if the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to a specific individual.
Consumer Rights	● **Affirmative Consent:** A controller shall not process a consumer's **sensitive data** without first obtaining the consumer's consent (or consent from a parent or guardian for processing personal data of a known child). ● **Opt Out Rights**: A consumer may opt out of the processing of personal data for the purposes of targeted advertising; sale of personal data; or profiling in furtherance of decisions that produce legal or similarly significant effects. Opt outs may be completed by an **authorized agent** or a **user-selected universal opt-out mechanism**. Specific procedural requirements apply to controllers that process data for targeted advertising. ● **Access:** A consumer has the right to confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data. ● **Correction:** A consumer has the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data. ● **Deletion:** A consumer has the right to delete personal data concerning the consumer. ● **Portability:** A consumer has the right to obtain personal data in a portable, and to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance. (Limit to two times per calendar year and includes a **trade secret exception**).
Business Obligations	● **Purpose specification:** A controller shall specify the express purposes for which personal data are collected and processed. ● **Data minimization:** A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed. ● **Avoid secondary use:** A controller shall not process personal data for purposes that are not reasonably

	necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent. ● **Security ("Duty of care"):** A controller shall take reasonable measures to secure personal data during both storage and use from unauthorized acquisition. Data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business. ● **Transparency:** A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes (1) the categories of personal data collected or processed by the controller or a processor; (2) the purposes for which the categories of personal data are processed; (3) how and where consumers may exercise their rights, including contact information and how to appeal; (4) the categories of personal data that the controller shares with third parties; (5) the categories of third parties with whom the controller shares personal data. ● **Avoid unlawful discrimination:** A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers. ● **Responding to consumer request:** Each controller shall establish a method for exercising consumer requests taking into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication, and the ability of the controller to authenticate the identity of the consumer making the request. A controller shall inform a consumer of any action taken on a request without undue delay and within 45 days of receipt of the request (may be extended by another 45 days where reasonably necessary). A controller shall further establish an internal process through which consumers may appeal a refusal to take action on a request and to inform a consumer of their ability to contact the Attorney General if the consumer has concerns about the results of an appeal.
Data Protection Assessments	● A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities that present a heightened risk of harm to a consumer. A controller shall make the data protection assessment available to the Attorney General upon request. A single data protection assessment may address a comparable set of processing operations that include similar activities.
Controller / Processor Distinction	● Yes. Provides in part that processing by a processor must be governed by a contract between the controller and processor that is binding on both parties and that sets out (a) processing instructions to which the processor is bound, including the nature and purpose of the processing, (b) the type of personal data subject to processing and duration of the processing, (c) requirements imposed by this Act, (d) provide for the deletion or return of data at the end of the provision of services; that the processor shall make available to the controller all information necessary to demonstrate compliance with the obligations under this Act; and reasonable audits.
Exceptions	● The CPA contains exceptions pertaining to de-identified and pseudonymous data; bona fide loyalty and other rewards programs; and to not restrict a controller or processor's ability to: (a) comply with laws, (b) comply with inquiries by government authorities, (c) cooperate in good faith with law enforcement, (d) exercise actual or anticipated legal claims, (e) conduct internal research to develop, improve, or repair products, services, or technology, (f) identify and repair technical errors that impair existing or intended functionality, (g) perform internal operations reasonably aligned with consumer expectations, (h) provide a product or service specifically requested by a consumer or perform a contract to which the consumer is a party, (i) protect vital interests of the consumer or another party, (j) prevent, detect, protect against, or respond to security incidents or illegal activity, (k) certain processing for public health reasons, (l) assist another person with activities in this subsection. ● The CPA carves out data maintained for employment record purposes and information subject to health privacy laws, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, COPPA, FERPA, data and financial institutions subject to GLBA.
Enforcement	● The CPA specifically states that it does **not provide the basis for a private right of action** for violations and that it **preempts** local laws. ● The CPA authorizes the Attorney General to conduct broad rulemaking and for the AG and district attorneys to bring actions seeking for civil penalties and injunctive relief. The CPA includes a **60-day opportunity to cure** that **sunsets on Jan. 1, 2025**.