Colorado Privacy Act

Overview of Business Obligations

The Colorado Privacy Act (CPA) and the Attorney General's accompanying regulations go into effect on July 1, 2023. The CPA governs how businesses, non-profits, and other entities handle Personal Data, or information linked or reasonably linkable to a Colorado resident. The CPA gives consumers rights with respect to their data and places obligations on entities covered under the CPA.

DOES THE CPA APPLY TO MY BUSINESS OR NON-PROFIT?

The CPA only applies to businesses, non-profit organizations, and certain public entities that meet specific threshold requirements:

1. Conducts business in Colorado or delivers commercial products or services targeted to residents of Colorado; AND either:
2. Processes the Personal Data of more than 100,000 individuals in any calendar year; or
3. Derives revenue or received discounts on goods or services in exchange for the sale of personal data of 25,000 or more individuals.

The CPA also applies to service providers, contractors, and vendors that manage, maintain, or provide services relating to the Personal Data on behalf of entities covered under the law.

WHO ISN'T COVERED UNDER THE CPA?

The CPA includes several exceptions at the entity- and information-level including HIPAA-covered entities, financial institutions subject to the Gramm-Leach-Bliley Act, information relating to an individual's credit rating, airlines, and others.

Note that the CPA does not apply to employment information or an individual's activities when acting in a commercial or employment context.

WHAT DOES IT MEAN TO "PROCESS" DATA?

The CPA broadly defines "Processing" data to include collecting, using, selling, storing, analyzing, deleting, modifying, disclosing or selling Personal Data. A Controller Processes data under the CPA even if it instructs another entity, like a service provider, to Process data on its behalf.

WHAT PRIVACY RIGHTS DO INDIVIDUALS HAVE UNDER THE CPA?

The CPA gives Colorado consumers several tools to learn how their Personal Data is collected, shared, and used:

1. ***Right to Opt-Out.*** Consumers can opt-out of the sale of their Personal Data and the use of their Personal Data for targeted advertising and certain types of profiling;
2. ***Right to Access.*** A consumer can request access to the Personal Data a Controller has collected about them, either directly from the Consumer or through other sources;

3. ***Right to Correct.*** A consumer can request a Controller to correct incorrect Personal Data the Controller maintains about them;
4. ***The Right to Delete.*** A Consumer can request that a Controller delete some or all Personal Data the Controller maintains about them; and
5. ***The Right to Portability.*** A Consumer can request a copy of the Personal Data a Controller maintains about them in a format that allows the transfer of that data to another platform.

WHAT DOES MY BUSINESS OR NON-PROFIT NEED TO DO TO COMPLY WITH THE CPA?

The CPA places several obligations on "Controllers," or entities that make decisions about the collection and processing of Personal Information. Mainly, a Controller must:

1. Post a privacy policy on its website;
2. Respond to consumers' data rights requests and requests to appeal the Controller's responses to data rights requests;
3. Only collect and store the Personal Data necessary for its business purposes;
4. Only collect and process Personal Data in the manner disclosed to consumers at the time of collection;
5. Use reasonable security practices to secure the Personal Data it maintains; and
6. Conduct Data Protection Assessments if the Controller conducts certain processing activities.

Controllers cannot:

1. Process "Sensitive Data" (biometric data, health information, etc.) without a consumer's consent; or
2. Use Personal Data in a way that would result in unlawful discrimination.

WHEN DOES MY BUSINESS OR NON-PROFIT NEED TO OBTAIN A CONSUMER'S CONSENT?

Controllers do not need to obtain consent to Process Personal Data in the manner that was disclosed to the consumer at the time of collection. But, Controllers do need to obtain consent in certain instances, including:

1. Collecting and Processing Sensitive Data;
2. Processing Personal Data for reasons other than those disclosed to consumers at the time of collection; and
3. Selling or processing Personal Data for targeted advertising after a consumer opted-out of such processing.

The CPA also places parameters on how and when Controllers may obtain consent. Controllers should be mindful about how their website provider presents consent choices to consumers because merely enabling default consent mechanisms may lead to violations of the CPA's consent requirements. For example, a consumer hovering over a pop-up banner or disregarding a pre-checked box is not affirmative or unambiguous consent. Moreover, the CPA prohibits a Controller from obtaining consent through deceptive webpage design, often called "dark patterns."

DOES MY BUSINESS OR NONPROFIT NEED TO CONDUCT A DATA PROTECTION ASSESSMENT?

A Controller conducts a Data Protection Assessment (DPA) to assess the risk of harm that its high-risk processing activities place on consumers. Under the CPA, a Controller must conduct a DPA when a processing activity presents a "heightened risk of harm" to consumers. A "heightened risk of harm" means:

1. Selling Personal Data;
2. Processing Sensitive Data;
3. Processing Personal Data for targeted advertising;
4. Processing Personal Data to profile consumers when the profiling presents a
    a. reasonably foreseeable risk of unfair treatment or an unlawful disparate impact on consumers;
    b. financial or physical injury to consumers;
    c. an offensive intrusion upon the solitude or seclusion or the private affairs of consumers; or
    d. poses other kinds of substantial injury to consumers.

The Attorney General can request a copy of the DPA at any time so it's important to conduct an accurate DPA, sufficiently document your reasoning in the DPA, and follow any processes or safeguards established in the DPA. Should a Controller to choose to change its high-risk data processing, it should conduct a new DPA.

WHAT OBLIGATIONS DOES MY BUSINESS HAVE AS A SERVICE PROVIDER?

The CPA refers to businesses as "Processors" when they maintain or process data at the instruction of Controllers. Depending on the types of products or services an entity provides, it may be a Processor or a Controller with respect to a specific activity.

It is not surprising that most Processor obligations center around their relationship with Controllers. The CPA enumerates many Processor obligations, but, namely, a Processor must:

1. Adhere to the processing instructions of the Controller.
2. Assist Controllers in meeting their obligations under the CPA. This includes implementing the technical and organizational measures necessary to do so.
3. Engage a subcontractor only after providing Controllers with an opportunity to object.
4. Protect the Personal Data they maintain and help Controllers respond to data breaches.
5. Include specific provisions in a binding contract between the Processor and the Controller addressing the responsibilities of each party according to their role, the processing instructions by which the Processor is bound, and audits.

WHAT IS A UNIVERSAL OPT-OUT MECHANISM?

The CPA requires a Controller to honor a consumer's opt-out request when communicated through a Universal Opt-Out Mechanism (UOOM), often thought of as an automated signal from a consumer's browser or device. While the California Attorney General has made this an existing

requirement under the California Privacy Protection Act, the CPA does not require Controllers to recognize UOOM signals until January 1, 2025.

WHO CAN ENFORCE VIOLATIONS UNDER THE CPA?

Only the Colorado Attorney General and District Attorneys may enforce CPA violations. Affected Colorado residents cannot enforce alleged violations.

The Attorney General must issue a notice to cure a violation before bringing an enforcement action if the Attorney General determines that a cure is possible. A cure may not be possible in instances where Sensitive Data has been sold without consent, for example, but is likely possible to fix a noncompliant privacy policy. A notice to cure gives the receiving entity 60 days to remedy the violation. This provision will sunset on January 1, 2025.

CPA violations are a deceptive trade practice under the Colorado Consumer Protection Act, affording the Attorney General and District Attorneys the ability to seek penalties of up to $20,000 per violation.

IS THE COLORADO ATTORNEY GENERAL ISSUING REGULATIONS UNDER THE CPA?

The Attorney General has rulemaking authority under the CPA and is currently in the rulemaking process. The Attorney General has released proposed rules and is accepting written feedback on the rules until mid-January. The proposed rules are detailed and address Controller and Processor obligations. The Attorney General will likely adopt the final rules sometime after holding a formal rulemaking hearing in early February.