MAYER | BROWN

July 8, 2021

Legal Update

Colorado's New Data Privacy Law: Comparing to Other States and Looking Ahead

Colorado has become the third state to enact a comprehensive consumer data privacy statute. Passed by the Colorado General Assembly on June 8, 2021, and signed into law by Colorado Governor Jared Polis on July 7, 2021, the Colorado Privacy Act ("CPA") is slated to come into effect on July 1, 2023. The CPA includes various key concepts that will be familiar for those who followed the California Consumer Privacy Act ("CCPA"), the California Privacy Rights Act ("CPRA"), and the Virginia Consumer Data Protection Act ("CDPA"). For companies subject to the CPA but otherwise new to comprehensive consumer data privacy legislation, the July 2023 effective date allows time to strengthen data governance frameworks.

Similar to Virginia's CDPA, Colorado's CPA adopts a nomenclature that is more aligned with the terminology used in the European Union's General Data Protection Regulation ("GDPR") than that used by California's CCPA and CPRA. While the CPA may present significant and new obligations for companies that have not previously undertaken a GDPR (or CDPA) analysis—or have not made these rights available at a global scale—companies that have implemented "global GDPR compliance programs" will likely not struggle to meet the requirements set out by the CPA.

Key CPA distinctions for companies to consider include the new and controversial "universal opt-out mechanism" for consumers (to be clarified in regulations), the opt-in consent requirement for "sensitive data," and the ability of district attorneys—in addition to the state attorney general—to enforce the statute.

What Should Companies Start Thinking About?

The threshold question for any company facing this new law is to determine whether the CPA is likely to apply to data that the company collects or processes. As detailed in the "Scope of the CPA" section below, the statute sets out a test based on the scale of a company's operations in regard to its control or processing of personal data.

Companies that are likely to be subject to the CPA should follow the office of the Colorado Attorney General (the "CO AG"), currently led by technology policy veteran Phil Weiser, as the CPA empowers his office with rulemaking capabilities. Possible rulemaking may include clarifying ambiguous definitions and addressing compliance concerns, for example as related to the "universal opt-out mechanism."

For companies already subject to the CCPA (and/or GDPR), there will be similarities to and overlap with certain compliance elements, including in the area of data subject rights. For companies that have not yet had to comply with the CCPA or GDPR but will be subject to the CPA, the time before July 2023 provides an

opportunity to conduct a data mapping and review of privacy/data governance programs. These efforts, as well as the implementation of attendant compliance programs, are a worthwhile investment, particularly as other state legislatures are actively considering comprehensive privacy laws of their own.

Scope of the CPA

The CPA applies to legal entities that conduct business in Colorado—or target Colorado residents—and that either (1) control or process personal data of more than 100,000 consumers per year, or (2) earn revenue from the sale of personal data and control or process personal data of more than 25,000 consumers. Similar to the CDPA and unlike the CCPA, the CPA does not have a minimum revenue threshold. Adopting GDPR nomenclature, the CPA refers to covered legal entities as "controllers."[1]

The CPA defines "consumer" narrowly as a Colorado resident acting only in an individual or household context, thus exempting employees and job applicants. Also, "personal data" is broadly defined as information that is linked or reasonably linkable to an identified or identifiable natural person, with exceptions for "de-identified data" and "publicly available information." The "de-identified data" exception is contingent on the controller taking certain measures to ensure that the data is not linkable to an individual and will not be re-identified.

In addition, the CPA exempts certain types of data and certain types of entities. Exempt entities include financial institutions subject to the Gramm-Leach-Bliley Act ("GLBA") and institutions of higher education. Exempt data include personal data subject to the GLBA, protected health information under the Health Insurance Portability and Accountability Act ("HIPAA"), personal information subject to the Fair Credit Reporting Act ("FCRA"), and data maintained for employment records purposes.

Comparing Exemptions in State Privacy Laws

EXEMPTION	CO CPA	VA CDPA	CA CCPA	CA CPRA
Financial institutions and data subject to GLBA	Both exempt	Both exempt	Institutions not exempt Data Exempt*	Institutions not exempt Data Exempt*
Covered entities/business associates and protected health data under HIPAA and HITECH	Data exempt	Both exempt	Limited entities exemption Data exempt*	Limited entities exemption Data exempt*
Personal information subject to FCRA	Exempt	Exempt	Exempt	Exempt
Employee/applicant personal data within employment context	Exempt	Exempt	Exempt from most obligations until 1/1/2023*	Exempt from most obligations until 1/1/2023*
Personal data within business (B2B) context	Exempt	Exempt	Exempt until 1/1/2023*	Exempt until 1/1/2023*
Non-profits	Not exempt	Exempt	Exempt	Exempt
Institutions of higher education	Exempt if non-profit	Exempt	Exempt if non-profit	Exempt if non-profit

* Subject to private right of action in the context of a data breach

Data Subject Rights Under the CPA

The CPA provides consumers with a variety of rights relating to personal data processed by controllers and processors, which consumers may request using methods specified by the controller in the required privacy notice.

Specifically, consumers have the right to the following:

- Right to opt out of processing[2] of personal data (for targeted advertising, sale of personal data, or profiling in furtherance of decisions "that produce legal or similarly significant effects concerning a consumer");
- Right to confirm whether a controller is processing a consumer's personal data and to access that data;
- Right to correct any inaccurate personal data;
- Right to delete personal data concerning the consumer;
- Right to data portability; and
- An appeals process for refusal of any data subject rights.

Universal Opt-out – Beginning on July 1, 2024, it will be mandatory for controllers that process personal data for purposes of targeted advertising or sale to offer a "universal opt-out mechanism" for consumers. The universal opt-out is unique to Colorado law, as the CCPA and CDPA have no similar requirement and the CPRA permits—but does not require—covered businesses to accept an "opt-out preference signal" as an alternative to offering opt-out links on their internet homepages. The CPA requires that the CO AG adopt rules regarding the technical specifications for such opt-out mechanisms by July 1, 2023.

While we do not yet know what these implementing rules will look like, the CPA sets out the framework for the universal opt-out mechanism:

- The manufacturer of any universal opt-out mechanism may not "unfairly disadvantage another controller";
- Controllers must inform consumers about opt-out options;
- Controllers must not have a default setting opt-out, but rather one that reflects "affirmative, freely given, and unambiguous choice to opt out";
- An opt-out mechanism must be consumer-friendly, clearly described, and easy to use;
- An opt-out mechanism must be as consistent as possible with any other, similar mechanism required by US law; and
- Controllers must be able to "accurately authenticate" the consumer as a Colorado resident and verify that the opt-out mechanism is a legitimate request.

Even if a consumer exercises their right through the universal opt-out, a business can rely on consent from the consumer to processing of data after presenting a "clear and conspicuous notice." Businesses relying on this exception must provide consumers with the ability to revoke their consent as easily as it was provided. The CPRA spells out similar requirements for its opt-out preference signal, which must be defined in regulations to be adopted by the CA AG by July 1, 2022. Given the similarities between CPRA and CPA rulemaking instructions, companies subject to the CPA should pay close attention to California's rulemaking as it unfolds over the next calendar year.

Non-discrimination – Controllers may not process personal data in violation of state or federal laws prohibiting unlawful discrimination against consumers.

45 day response to requests – Controllers must acknowledge action "without undue delay" and within 45 days after receipt of a consumer request. The controller may extend the response period for an

additional 45 days. The controller must also inform the consumer "without undue delay" and within 45 days if not taking action on a consumer request, the reasons for not taking action, and instructions for how to appeal the decision.

Cost of compliance – Controllers must comply with a first consumer request free of charge, but can charge for additional requests within a 12 month period based on a formula provided in the CPA.

Authentication – Controllers may request additional information as "reasonably necessary to authenticate the request" if unable to do so using commercially reasonable efforts.

Consumer right to appeal – Controllers must establish an appeals process for consumers to appeal the refusal to take action on a request under any of the rights provided by the CPA. This appeals process must be "conspicuously available and as easy to use" as the process for submitting a request. The controller must respond to a consumer within 45 days, but may extend by an additional 60 days. Controllers must also inform consumers of their ability to contact the CO AG with any concerns about the result of an appeal under this section.

Comparing Consumer Rights under State Privacy Laws

KEY DISTINCTIONS IN BOLD

DATA SUBJECT RIGHTS	CO CPA	VA CDPA	CA CCPA	CA CPRA
Access	Yes	Yes	Yes	Yes
Correct	**Yes**	Yes	**No**	Yes
Delete	Yes (personal data concerning the customer)	Yes (data provided by or obtained about consumer)	Yes (data collected from consumer)	Yes (data collected from consumer)
Portability	Yes	Yes	Yes	Yes
Opt-out of sale	Yes	Yes	Yes	Yes
Non-discrimination	Yes	Yes	Yes	Yes
Appeals process	**Yes**	Yes	**No**	**No**

Controller and Business-Related Obligations

Under the CPA, controllers have the following additional duties and obligations:

- **Transparency** –
  a) Provide consumers with a "reasonably accessible, clear, and meaningful privacy notice" that includes (1) categories of personal data collected or processed by the controller or a processor; (2) purposes for processing of personal data; (3) how and where consumers may exercise rights under the CPA, including controller contact information and how to appeal a controller response; (4) categories of personal data a controller shares with third parties; and (5) categories of third parties with whom the controller shares data.*
  b) Any sale or processing for targeted advertising of personal data must be "clearly and conspicuously" disclosed, as well as information on how a consumer may opt out.

c) Controllers may not (i) require creation of a new account to exercise a right, or (ii) increase cost or decrease availability of a product or service based on exercise of a right.

d) Does not restrict the ability of a controller to provide a different product or service offering involving personal data if related to "a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discount, or club card program."

* The CCPA and CPRA require similar disclosures; however, they compel disclosure of the categories of personal information sold only in response to a consumer access request.

- **Purpose specification** – Specify express purposes for collecting and processing personal data.
- **Data minimization** – Collection of personal data should be limited to data that is "adequate, relevant, and limited to what is reasonable necessary" for the specified purposes of processing.
- **Secondary use** – Absent prior consumer consent, personal data should not be processed for purposes that are "not reasonably necessary to or compatible with the specified purposes" for processing. For example, this limits a business from sharing or using information provided solely for the purpose of billing or order completion for the purpose of targeted advertising.
- **Security requirements** – Reasonable measures must be taken to secure personal data from unauthorized use, "appropriate to the volume, scope, and nature of the personal data processed and the nature of the business."
- **Consent to process sensitive data** – Obtain consent from consumers (or parent or lawful guardian in the case of a known child under 13 years of age) for the processing of their sensitive data. "Sensitive data" includes (1) racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; (2) genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or (3) personal data from a known child. While Virginia's CDPA requires that processing of sensitive data comply with the federal Children's Online Privacy Protection Act (COPPA), the CPA does not implement this additional requirement. The CPA exempts data of a minor handled in a manner compliant with COPPA from the CPA's requirements.
- **Data protection assessments** – Starting on July 1, 2023, requirement of a data protection assessment for data processing activity involving personal data acquired on or after that date that presents "heightened risk of harm to a consumer." Such activities include (1) processing personal data for targeted advertising or certain kinds of profiling that could negatively impact consumers; (2) sale of personal data; and (3) processing of sensitive data. The CPA sets forth considerations for such a data protection assessment, and requires that the data protection assessment be made available to the CO AG upon request. A single data protection assessment may be prepared for a "comparable set of processing operations that include similar activities."
- **De-identified data** – For data or a device that cannot reasonably be linked to or identify an individual, a controller must (1) take reasonable measures to ensure that the data cannot be associated with an individual; (2) publicly commit to maintain and use the de-identified data as is and not attempt to re-identify it; and (3) contractually obligate any data recipient to comply with the same. Under the CPA, controllers and processors are not required to re-identify de-identified data solely to comply with the law.

Data Controller Obligations under State Privacy Laws

KEY DISTINCTIONS IN BOLD

CONTROLLER OBLIGATIONS	CO CPA	VA CDPA	CA CCPA	CA CPRA
Data minimization	**Yes**	Yes	**No**	Yes
Purpose limitation	Yes	Yes	Yes	Yes
Security requirements	**Yes**	Yes	**No, but the private right of action applies to security breaches**	Yes
Consent for sensitive data	**Yes**	Yes	**No**	**No, consumers can limit use to what is reasonably necessary**
Special requirements for children's data	Yes (personal data for a known child under 13 years of age)	Yes (sensitive data of children under 13 years of age)	Yes (sale of personal information of children under 16 years of age and under 13 years of age)	Yes (sale of personal information of children under 16 years of age and under 13 years of age)
Privacy notice	Yes	Yes	Yes	Yes
Disclose sale	Yes	Yes	Yes	Yes
Data protection assessment	**Yes, available upon request by CO AG.**	Yes	**No**	Yes, risk assessments submitted to CA Privacy Protection Agency
Requirements for de-identified data	Yes	Yes	Yes	Yes

Processor Obligations

The CPA also sets forth certain requirements for "processors,"[3] namely that a processor must follow the controller's instructions and assist the controller in meeting certain of its CPA obligations.

The CPA requires a binding contract between a controller and a processor governing the processor's data processing procedures in which the following obligations must be included. These obligations align more closely with GDPR and the CDPA's contractual requirements for processors than with the CCPA's contractual requirements for service providers.

- Appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between controller and processor to implement the measures;
- Instructions for processing data, the nature and purpose of processing, the type of data subject to processing, and the duration of processing;
- Duty of confidentiality for each person processing personal data;
- Deletion or return of all personal data to the controller, at the controller's discretion, at the end of the provision of services, unless retention is required by law;

- Making available to the controller all information necessary to demonstrate the processor's CPA compliance;
- Cooperation with reasonable audits and inspections by the controller or the controller's designated auditor, or an arrangement for a qualified and independent audit; and
- Requiring via a written contract any subcontractor to meet the obligations of the processor with respect to the personal data, and providing the controller an opportunity to object.

These contractual requirements for processors closely resemble GDPR and the CDPA; absent significant rulemaking, companies undertaking re-contracting initiatives to comply with these existing frameworks are not likely to have to make material changes to account for the CPA.

Implementation

Like the CCPA and CPRA, and unlike the CDPA, which calls for the creation of a "work group," the CPA authorizes rulemaking authority for implementing the law. The CO AG may promulgate rules to implement the CPA; specific rules regarding the universal opt-out mechanism for consumers are due by July 1, 2023.

Enforcement

Like the CDPA, and unlike the CCPA and CPRA, which contain a limited private right of action for data breaches, the CPA does not provide a private right of action. The CPA specifies that a violation is a deceptive trade practice and that the CO AG and district attorneys have exclusive enforcement authority. The CPA is the first state data privacy law that provides district attorneys with enforcement authority. Prior to an enforcement action, the CO AG or district attorney will issue a notice of violation to the controller if a cure is deemed possible. Then, if a controller fails to cure the violation within 60 days, an action may be brought. However, this generous cure provision is temporary; it will be repealed, effective January 1, 2025. A controller or processor that violates the provisions of the CPA is subject to civil penalty and may be enjoined from further violations.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Vivek K. Mohan
+1 650 331 2054
vmohan@mayerbrown.com

Joshua M. Cohen
+1 312 701 8198
jmcohen@mayerbrown.com

Evan M. Wooten
+1 213 621 9450
ewooten@mayerbrown.com

Anjani D. Nadadur
+1 202 263 3284
anadadur@mayerbrown.com

Endnotes

[1] A "controller" is defined in the CPA as "a person that, alone or jointly with others, determines the purposes and means of processing personal data."

[2] "Process" or "processing" is defined in the CPA as "the collection, use, sale, storage, disclosure, analysis, deletion, or modification of personal data and includes the actions of a controller directing a processor to process personal data."

[3] A "processor" is defined in the CPA as "a person that processes personal data on behalf of a controller."