Published on *The National Law Review* https://natlawreview.com

And Now There are Three …. The Colorado Privacy Act

Article By:

Cynthia J. Larose

Christopher J. Buontempo

Colorado has now joined California and Virginia to become the third US state to pass a comprehensive data privacy legislation when Governor Jared Polis signed the Colorado Privacy Act (the "CPA") into law on July 8, 2021. The new law is set to take effect on July 1, 2023.

The CPA borrows in part from the European Union's General Data Protection Regulation ("GDPR"), but more significantly from both the California Consumer Privacy Act ("CCPA", including as amended by the California Privacy Rights Act ("CPRA")), and the Virginia Consumer Data Protection Act ("VCDPA"). Below, we highlight some of the CPA's key elements and explore how the law compares to the CCPA and VCDPA.

Applicability:

The CPA applies to companies that conduct business in Colorado or sell product or services intentionally targeted to residents of Colorado, and meet **either** of the following thresholds: (i) controls or processes personal data of 100,000 or more consumers during a calendar year; or (ii) derive revenue or receive discounts from the sale of personal data and control or process data of at least 25,000 consumers.

Applicability of the CPA is very similar to the VCDPA, with the caveat that the VCDPA also requires that businesses must also derive over 50% of their gross revenue from the sale of personal data to meet the second applicability threshold noted above. The applicability of the CPA is narrower in most instances than the CCPA, but is slightly different – so there will be some business that fall within CCPA's purview, but not CPA's, and vice versa. The CCPA contains a revenue threshold of $25M annual revenue, but **the CPA does not contain a revenue threshold at all**, and the CPA's 100,000 consumer threshold is double the CCPA's 50,000.

Exemptions:

The CPA does not apply to individuals acting in a commercial or employment context, and does not apply to job applicants. Similar to CCPA, the CPA does not apply to protected health information and certain other healthcare information (though it does not contain an entity-wide exemption, as the

CCPA and VCDPA provide), information subject to certain federal laws such as FCRA, GLBA, COPPA, FERPA. However, unlike the CCPA and VCDPA, **the CPA does not contain an exemption for non-profit organizations**.

Terminology

Similar to the VCDPA, **the CPA uses GDPR-style terminology**. For those familiar with the CCPA but not the GDPR, where the CCPA uses "business," the CPA uses "controller." Instead of the CCPA term "service provider," the CPA uses "processor." In effect, the terms are very similar and can be used interchangeably in most cases.

The definition of "sale" in the CPA is nearly identical to the CCPA definition, and includes any exchange for monetary *or other valuable consideration*. The VCDPA defines "sale" more narrowly, including only exchanges for monetary consideration.

Consumer Rights

Right to Opt-Out. Under the CPA, consumers may opt out of the processing of their personal data for: (i) targeted advertising; (ii) the sale of personal data; and (iii) profiling in further of decisions that produce legal or similarly significant effects concerning a consumer (provision or denial of financial, lending, housing, insurance, education, criminal justice, employment, healthcare, or essential goods or services). The CPA requires that controllers provide a "clear and conspicuous" method to exercise the right to opt-out of the sale of personal data or targeted advertising, which must be in the controller's privacy notice as well as in a readily accessible location outside the privacy notice. Controllers may also allow users to opt-out through a universal opt-out mechanism that meets technical specifications established by the Attorney General (this becomes mandatory on July 1, 2024).

Right of access. Consumers have the right to confirm whether a controller is processing their personal data and to access that data.

Right to correction. Consumers have the right to correct inaccuracies in their personal data.

Right to deletion. Consumers have the right to delete their personal data.

Right to data portability. Up to two (2) times per calendar year, consumers have the right to obtain their personal data in a portable and readily usable format that allows the consumer to transmit the data to another entity "without hindrance."

Consumer rights under the CPA are nearly identical to those established by the VCDPA. They are also very similar to those under the CCPA, however, **the CPA's opt-out rights are broader than the CCPA with respect to targeted advertising and profiling in further of decisions that produce legal or similarly significant effects.**

Fulfilling Consumer Requests

Under the CPA, controllers have 45 days to fulfill consumer requests (which may be extended another 45 days where reasonably necessary). These timelines are in line with the CCPA and the VCDPA.

Privacy Notice Required Disclosures

The CPA's privacy notice required disclosures are nearly identical to those required by the VCDPA, requiring that controllers provide a reasonably accessible, clear and meaningful privacy notice that includes: (i) the categories of personal data collected or processed; (ii) the purposes for processing of personal data; (iii) how and where consumers may exercise their rights and how to appeal a controller's action in response to a request; (iv) categories of personal data shared with third parties; and (v) the categories of third parties with whom the controller shares personal data.

If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose the sale or processing, as well as the manner in which a consumer may exercise the right to opt out of the sale or processing.

Other Processing Obligations

Similar to the VCDPA (and similar the CCPA as amended by the California Privacy Rights Act), the CPA creates the following duties for controllers: (i) transparency; (ii) purpose specification; (iii) data minimization; (iv) avoid secondary use of personal data; (v) duty of care; (vi) avoid unlawful discrimination; and (vii) process sensitive data only with consumer consent.

It is important to note here that the C**PA uses a heightened "consent" standard that is similar to the standard used by the CPRA. "Consent" under the CPA means "*a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data*."** The CPA states that following does not constitute "consent": (a) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; (b) hovering over, muting, pausing, or closing a given piece of content; and (c) agreement obtained through dark patterns (a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice).

Data Protection Assessments

Similar to the CPRA and the VCDPA, the CPA requires that controllers conduct a data protection assessment when processing personal data that presents a heightened risk of harm to a consumer. This includes processing sensitive data, selling personal data, and processing personal data for targeted advertising or profiling that presents a reasonably foreseeable risk of:

- Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
- Financial or physical injury to consumers;
- A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or
- Other substantial injury to consumers.

Additionally, **controllers must make the assessments available to the Attorney General upon**

request.

Engaging Processors

Requirements under the CPA for engaging processors is similar in many respect with the VCDPA and to the CCPA as amended by the CPRA.

The CPA requires processors to adhere to controller instructions and assist the controller in meeting its obligations under the CPA, including the fulfillment of consumer requests, notification of security breaches, and data protection impact assessments. Processors must also allow reasonable audits and inspections by the controller.

Under the CPA, processors must ensure that each of their subprocessors is subject to a duty of confidentiality, and similar to the GDPR, but unlike the CCPA and the VCDPA, controllers have the right to object to any subprocessors.

Similar to the VCDPA, and to the CCPA and CPRA in some respects, contracts between controllers and processors under the CPA must be in writing and set forth (i) the processing instructions including the nature and purpose of the processing; (ii) the type of personal data and duration of the processing; and (iii) obligations to delete or return all personal data at the end of the services period.

To the extent that a controller provides anonymized data to a processor (or other third party in general), the CPA requires that the processor or third party is contractually required to take reasonable measures to ensure that the anonymized data cannot be associated with an individual, and does not attempt to re-identify the data.

Enforcement

Similar to the VCDPA and to the CCPA (other than in the context of data breaches), the CPA does not create a private right of action. Enforcement is exclusively with the Attorney General and District Attorneys. A violation of the CPA is considered a deceptive trade practice under the Colorado Consumer Protection Act.

Until January 1, 2025, prior to any enforcement of the CPA, controllers must be given a 60 day cure period (where a cure is deemed possible by the Attorney General or District Attorney). The CCPA and the VCDPA also provide for cure periods, though those are not set to sunset as is provided under the CPA.

Colorado has now joined California and Virginia to become the third US state to pass a comprehensive data privacy legislation when Governor Jared Polis signed the Colorado Privacy Act (the “CPA”) into law on July 8, 2021. The new law is set to take effect on July 1, 2023.

The CPA borrows in part from the European Union’s General Data Protection Regulation (“GDPR”), but more significantly from both the California Consumer Privacy Act (“CCPA”, including as amended by the California Privacy Rights Act (“CPRA”)), and the Virginia Consumer Data Protection Act (“VCDPA”). Below, we highlight some of the CPA’s key elements and explore how the law compares to the CCPA and VCDPA.

Applicability:

The CPA applies to companies that conduct business in Colorado or sell product or services intentionally targeted to residents of Colorado, and meet **either** of the following thresholds: (i) controls or processes personal data of 100,000 or more consumers during a calendar year; or (ii) derive revenue or receive discounts from the sale of personal data and control or process data of at least 25,000 consumers.

Applicability of the CPA is very similar to the VCDPA, with the caveat that the VCDPA also requires that businesses must also derive over 50% of their gross revenue from the sale of personal data to meet the second applicability threshold noted above. The applicability of the CPA is narrower in most instances than the CCPA, but is slightly different – so there will be some business that fall within CCPA's purview, but not CPA's, and vice versa. The CCPA contains a revenue threshold of $25M annual revenue, but **the CPA does not contain a revenue threshold at all**, and the CPA's 100,000 consumer threshold is double the CCPA's 50,000.

Exemptions:

The CPA does not apply to individuals acting in a commercial or employment context, and does not apply to job applicants. Similar to CCPA, the CPA does not apply to protected health information and certain other healthcare information (though it does not contain an entity-wide exemption, as the CCPA and VCDPA provide), information subject to certain federal laws such as FCRA, GLBA, COPPA, FERPA. However, unlike the CCPA and VCDPA, **the CPA does not contain an exemption for non-profit organizations**.

Terminology

Similar to the VCDPA, **the CPA uses GDPR-style terminology**. For those familiar with the CCPA but not the GDPR, where the CCPA uses "business," the CPA uses "controller." Instead of the CCPA term "service provider," the CPA uses "processor." In effect, the terms are very similar and can be used interchangeably in most cases.

The definition of "sale" in the CPA is nearly identical to the CCPA definition, and includes any exchange for monetary *or other valuable consideration*. The VCDPA defines "sale" more narrowly, including only exchanges for monetary consideration.

Consumer Rights

Right to Opt-Out. Under the CPA, consumers may opt out of the processing of their personal data for: (i) targeted advertising; (ii) the sale of personal data; and (iii) profiling in further of decisions that produce legal or similarly significant effects concerning a consumer (provision or denial of financial, lending, housing, insurance, education, criminal justice, employment, healthcare, or essential goods or services). The CPA requires that controllers provide a "clear and conspicuous" method to exercise the right to opt-out of the sale of personal data or targeted advertising, which must be in the controller's privacy notice as well as in a readily accessible location outside the privacy notice. Controllers may also allow users to opt-out through a universal opt-out mechanism that meets technical specifications established by the Attorney General (this becomes mandatory on July 1, 2024).

Right of access. Consumers have the right to confirm whether a controller is processing their personal data and to access that data.

Right to correction. Consumers have the right to correct inaccuracies in their personal data.

Right to deletion. Consumers have the right to delete their personal data.

Right to data portability. Up to two (2) times per calendar year, consumers have the right to obtain their personal data in a portable and readily usable format that allows the consumer to transmit the data to another entity "without hindrance."

Consumer rights under the CPA are nearly identical to those established by the VCDPA. They are also very similar to those under the CCPA, however, **the CPA's opt-out rights are broader than the CCPA with respect to targeted advertising and profiling in further of decisions that produce legal or similarly significant effects.**

Fulfilling Consumer Requests

Under the CPA, controllers have 45 days to fulfill consumer requests (which may be extended another 45 days where reasonably necessary). These timelines are in line with the CCPA and the VCDPA.

Privacy Notice Required Disclosures

The CPA's privacy notice required disclosures are nearly identical to those required by the VCDPA, requiring that controllers provide a reasonably accessible, clear and meaningful privacy notice that includes: (i) the categories of personal data collected or processed; (ii) the purposes for processing of personal data; (iii) how and where consumers may exercise their rights and how to appeal a controller's action in response to a request; (iv) categories of personal data shared with third parties; and (v) the categories of third parties with whom the controller shares personal data.

If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose the sale or processing, as well as the manner in which a consumer may exercise the right to opt out of the sale or processing.

Other Processing Obligations

Similar to the VCDPA (and similar the CCPA as amended by the California Privacy Rights Act), the CPA creates the following duties for controllers: (i) transparency; (ii) purpose specification; (iii) data minimization; (iv) avoid secondary use of personal data; (v) duty of care; (vi) avoid unlawful discrimination; and (vii) process sensitive data only with consumer consent.

It is important to note here that the C**PA uses a heightened "consent" standard that is similar to the standard used by the CPRA. "Consent" under the CPA means "*a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data*."** The CPA states that following does not constitute "consent": (a) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; (b) hovering over, muting, pausing, or closing a given piece of content; and (c) agreement obtained through dark patterns (a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice).

Data Protection Assessments

Similar to the CPRA and the VCDPA, the CPA requires that controllers conduct a data protection assessment when processing personal data that presents a heightened risk of harm to a consumer. This includes processing sensitive data, selling personal data, and processing personal data for targeted advertising or profiling that presents a reasonably foreseeable risk of:

- Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
- Financial or physical injury to consumers;
- A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or
- Other substantial injury to consumers.

Additionally, **controllers must make the assessments available to the Attorney General upon request.**

Engaging Processors

Requirements under the CPA for engaging processors is similar in many respect with the VCDPA and to the CCPA as amended by the CPRA.

The CPA requires processors to adhere to controller instructions and assist the controller in meeting its obligations under the CPA, including the fulfillment of consumer requests, notification of security breaches, and data protection impact assessments. Processors must also allow reasonable audits and inspections by the controller.

Under the CPA, processors must ensure that each of their subprocessors is subject to a duty of confidentiality, and similar to the GDPR, but unlike the CCPA and the VCDPA, controllers have the right to object to any subprocessors.

Similar to the VCDPA, and to the CCPA and CPRA in some respects, contracts between controllers and processors under the CPA must be in writing and set forth (i) the processing instructions including the nature and purpose of the processing; (ii) the type of personal data and duration of the processing; and (iii) obligations to delete or return all personal data at the end of the services period.

To the extent that a controller provides anonymized data to a processor (or other third party in general), the CPA requires that the processor or third party is contractually required to take reasonable measures to ensure that the anonymized data cannot be associated with an individual, and does not attempt to re-identify the data.

Enforcement

Similar to the VCDPA and to the CCPA (other than in the context of data breaches), the CPA does not create a private right of action. Enforcement is exclusively with the Attorney General and District Attorneys. A violation of the CPA is considered a deceptive trade practice under the Colorado

Consumer Protection Act.

Until January 1, 2025, prior to any enforcement of the CPA, controllers must be given a 60 day cure period (where a cure is deemed possible by the Attorney General or District Attorney). The CCPA and the VCDPA also provide for cure periods, though those are not set to sunset as is provided under the CPA.

National Law Review, Volume XI, Number 197