GIBSON DUNN

July 9, 2021

THE COLORADO PRIVACY ACT: ENACTMENT OF COMPREHENSIVE U.S. STATE CONSUMER PRIVACY LAWS CONTINUES

To Our Clients and Friends:

On July 7, 2021, Colorado Governor Jared Polis signed into law the Colorado Privacy Act ("CPA"), making Colorado the third state to pass comprehensive consumer privacy legislation, following California and Virginia.

The CPA will go into effect on July 1, 2023.[1] In many ways, the CPA is similar—but not identical—to the models set out by its California and Virginia predecessors the California Consumer Privacy Act ("CCPA"), the California Privacy Rights Enforcement Act ("CPRA") and the Virginia Consumer Data Protection Act ("VCDPA"). The CPA will grant Colorado residents the right to access, correct, and delete the personal data held by organizations subject to the law. It also will give Colorado residents the right to opt-out of the processing of their personal data for purposes of targeted advertising, sale of their personal data, and profiling in furtherance of decisions that produce legal or similarly significant effects on the consumer. In ensuring that they are prepared to comply with the CPA, many companies should be able to build upon the compliance measures they have developed for the California and Virginia laws to a significant extent.

The CPA does, however, contain a few notable distinctions when compared to its California and Virginia counterparts. First, the CPA applies to nonprofit entities that meet certain thresholds described more fully below, whereas the California and Virginia laws exempt nonprofit organizations. Similar to the VCDPA and unlike the CPRA—the California law slated to replace the CCPA in 2023—the CPA does not apply to employee or business-to-business data. Like the VCDPA, the CPA will not provide a private right of action.[2] Instead, it is enforceable only by the Colorado Attorney General or state district attorneys. The laws in all three states differ with respect to the required process for responding to a consumer privacy request and the applicable exceptions for responding to such requests.

Finally, in addition to adopting certain terminology such as "personal data," "controller" and "processor," most commonly used in privacy legislation outside the United States, the CPA applies certain obligations modeled after the European Union's General Data Protection Regulation ("GDPR"), including the requirement to conduct data protection assessments. Further, the CPA imposes certain obligations on data processors, including requirements to assist the controller in meeting its obligations under the statute and to provide the controller with audit rights, deletion rights, and the ability to object to subprocessors. Companies that have undergone GDPR compliance work thus will have a leg up with respect to these obligations.

The CPA gives the Attorney General rulemaking authority to fill some notable gaps in the statute. Among them are how businesses should implement the requirement that consumers have a universal mechanism to easily opt out of the sale of their personal data or its use for targeted advertising, which must be implemented by July 1, 2023. In addition, as Governor Polis noted in a signing statement, the Colorado General Assembly already is engaged in conversations around enacting "clean-up" legislation to further refine the CPA.[3]

The following is a detailed overview of the CPA's provisions.

I. CPA's Key Rights and Provisions

A. Scope of Covered Businesses, Personal Data, and Exemptions

1. *Who Must Comply with the CPA?*

The CPA applies to any legal entity that "conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado" and that satisfies one or both of the following thresholds:

1. During a calendar year, controls or processes personal data of 100,000 or more Colorado residents; or

2. Both derives revenue or receives discounts from selling personal data and processes or controls the personal data of 25,000 or more Colorado residents.[4]

In other words, the CPA will likely apply to companies that interact with Colorado residents, or process personal data of Colorado residents on a relatively large scale, including non-profit organizations. Like the California and Virginia laws, the CPA does not define what it means to "conduct business" in Colorado. However, in the absence of further guidance from the Attorney General, businesses can assume that economic activity that triggers tax liability or personal jurisdiction in Colorado likely will trigger CPA applicability.

Notably, like the VCDPA (and unlike the CCPA), the statute does not include a standalone revenue threshold for determining applicability separate from the above thresholds regarding contacts with Colorado. Therefore, even large businesses will not be subject to the CPA unless they fall within one of the two categories above, which focus on the number of Colorado residents affected by the business's processing or control of personal data.

The CPA contains a number of exclusions, including both entity-level and data-specific exemptions. For instance, it does not apply to certain entities, including air carriers[5] and national securities associations.[6] Employment records and certain data held by public utilities, state government, and public institutions of higher education are also exempt.[7] The CPA also exempts data subject to various state and federal laws and regulations, including the Gramm-Leach-Bliley Act ("GLBA"), Health Insurance Portability and Accountability Act ("HIPAA"), Fair Credit Reporting Act ("FCRA"), and the Children's Online Privacy Protection Act ("COPPA").[8] Like the California and Virginia laws,

however, these latter exemptions do not apply at the entity level and instead only apply to data that is governed by and processed in accordance with such laws.

The CPA also explicitly exempts a wide variety of activities in which controllers and processors might engage, such as responding to identity theft, protecting public health, or engaging in internal product-development research.[9]

2. *Definition of "Personal Data" and "Sensitive Data"*

The CPA defines personal data as "information that is linked or reasonably linkable to an identified or identifiable individual," but excludes "de-identified data or publicly available information."[10] The CPA defines "publicly available information" as information that is "lawfully made available from federal, state, or local government records" or that "a controller has a reasonable basis to believe the consumer has lawfully made available to the general public."[11] The CPA further does not apply to data "maintained for employment records purposes."[12]

As discussed below, opt-out rights apply to certain processing of personal data, while opt-in consent must be obtained prior to processing categories of data that are "sensitive." The statute defines "sensitive data" to mean "(a) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; (b) genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or (c) personal data from a known child."[13]

B. Consumer Rights Under the Colorado Privacy Act

A "consumer" under the CPA is a Colorado resident who is "acting only in an individual or household context."[14] Like the VCDPA, the CPA expressly exempts individuals acting in a "commercial or employment context," such as a job applicant, from the definition of "consumer."[15] This contrasts with the CPRA, which does not exempt business-to-business and employee data, and the CCPA's exemptions for such data that are set to expire in 2023.

1. *Access, correction, deletion, and data portability rights*

The CPA gives Colorado consumers the right to access, correct, delete, or obtain a copy of their personal data in a portable format.[16]

Controllers must provide consumers with "a reasonably accessible, clear, and meaningful privacy notice."[17] Those notices must tell consumers what types of data controllers collect, how they use it and what personal data is shared with third parties, with whom they share it, and "how and where" consumers can exercise their rights.[18]

To exercise their rights over their personal data, consumers must submit a request to the controller.[19] Controllers cannot require consumers to create an account to make a request about their data,[20] and they also cannot discriminate against consumers for exercising their rights, such as by

increasing prices or reducing access to products or services.[21] However, they can still offer discounts and perks that are part of loyalty and club-card programs.[22]

2. *Right to opt-out of sale of personal data, targeted advertising, and profiling*

As under the VCDPA, under the CPA consumers have the right to opt out of the processing of their non-sensitive personal data for purposes of targeted advertising, the sale of personal data, or "profiling in furtherance of decisions that produce legal or similarly significant effects."[23] The CPA, like the CCPA, adopts a broad definition of "sale" of personal data to mean "the exchange of personal data for *monetary or other valuable* consideration by a controller to a third party."[24] However, the CPA contains some broader exemptions from the definition of "sale" than the CCPA, including for the transfer of personal data to an affiliate or to a processor or when a consumer directs disclosure through interactions with a third party or makes personal data publicly available.[25]

If the controller sells personal data or uses it for targeted advertising, the controller's privacy notice must "clearly and conspicuously" disclose that fact and how consumers can opt out.[26] In addition, controllers must provide that opt-out information in a "readily accessible location outside the privacy notice."[27] However, the CPA, like the VCDPA, does not specify how controllers must present consumers with these opt-out rights.

The CPA permits consumers to communicate this opt out through technological means, such as a browser or device setting.[28] By July 1, 2024, consumers must be allowed to opt out of the sale of their data or its use for targeted advertising through a "user-selected universal opt-out mechanism."[29] Opting-out of profiling, however, does not appear to be explicitly addressed by this mechanism. Exactly what the universal opt-out mechanism will look like will be up to the Attorney General, who will be tasked with defining the technical requirements of such a mechanism by July 1, 2023.[30]

3. *New rights to opt-in to the processing of "sensitive" data and to appeal*

a. Right to opt-in to the processing of "sensitive" data"

Similar to the VCDPA, controllers must first obtain a consumer's opt-in consent before processing "sensitive data," which includes children's data; genetic or biometric data used to uniquely identify a person; and "personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status."[31] Unlike the VCDPA, however, the CPA does not define "biometric" data.

Consent can be given only with a "clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement," such as an electronic statement.[32] Like its California counterparts, the CPA further specifies that consent does not include acceptance of broad or general terms, "hovering over, muting, pausing, or closing a given piece of content," or consent obtained through the use of "dark patterns," which are "user interface[s] designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice."[33]

b. Right to appeal

Like its counterparts, the CPA provides that controllers must respond to requests to exercise the consumer rights granted by the statute within 45 days, which the controller may extend once for an additional 45-day period if it provides notice to the requesting consumer explaining the reason for the delay.[34] A controller cannot charge the consumer for the first such request the consumer makes in any one-year period, but can charge for additional requests in that year. [35] The CPA, like the VCDPA (but unlike the CCPA/CPRA), requires controllers to establish an internal appeals process for consumers when the controller does not take action on their request.[36] The appeals process must be "conspicuously available and as easy to use as the process for submitting the request."[37] Once controllers act on the appeal—which they must do within 45 days, subject to an additional extension of 60 days if necessary—they must also tell consumers how to contact the Attorney General's Office if the consumer has concerns about the result of the appeal.[38]

C. Business Obligations

1. *Data Minimization and technical safeguards requirements*

Like the California and Virginia laws, the CPA limits businesses' collection and use of personal data and requires the implementation of technical safeguards.[39] The CPA explicitly limits the collection and processing by controllers of personal data to that which is reasonably necessary and compatible with the purposes previously disclosed to consumers.[40] Relatedly, controllers must obtain consent from consumers before processing personal data collected for another stated purpose.[41] Also, under the CPA controllers and processors must take reasonable measures to keep personal data confidential and to adopt security measures to protect the data from "unauthorized acquisition" that are "appropriate to the volume, scope, and nature" of the data and the controller's business.[42]

2. *GDPR-like requirements – data protection assessments, data processing agreements, restrictions on processing personal data*

The CPA, like the VCDPA, requires controllers to conduct "data protection assessments," similar to the data protection impact assessments required under the GDPR, to evaluate the risks associated with certain processing activities that pose a heightened risk – such as those related to sensitive data and personal data for targeted advertising and profiling that present a reasonably foreseeable risk of unfair or deceptive treatment or unlawful disparate impact to consumers – and the sale of personal data.[43] Unlike the GDPR, however, the CPA does not specify the frequency with which these assessments must occur. The CPA requires controllers to make these assessments available to the Attorney General upon request.[44]

The CPA also requires controllers and processors to contractually define their relationship. These contracts must include provisions related to, among other things, audits of the processor's actions and the confidentiality, duration, deletion, and technical security requirements of the personal data to be processed.[45]

D. Enforcement

The CPA is enforceable by Colorado's Attorney General and state district attorneys, subject to a 60-day cure period for any alleged violation until 2025 (in contrast to the 30-day cure period under the CCPA and VCDPA and the CPRA's elimination of any cure period).[46] Local laws are pre-empted and consumers have no private right of action.[47] A violation of the CPA constitutes a deceptive trade practice for purposes of the Colorado Consumer Protection Act, with violations punishable by civil penalties of up to $20,000 per violation (with a "violation" measured per consumer and per transaction).[48] The Attorney General or district attorney may enforce the CPA by seeking injunctive relief.

In addition to rulemaking authority to specify the universal opt-out mechanism, the Colorado Attorney General is authorized to "adopt rules that govern the process of issuing opinion letters and interpretive guidance to develop an operational framework for business that includes a good faith reliance defense of an action that may otherwise constitute a violation" of the CPA.[49]

* * * *

As we counsel our clients through GDPR, CCPA, CPRA, VCDPA, and CPA compliance, we understand what a major undertaking it is and has been for many companies. As discussed above, the CPA resembles the VCDPA in several respects, including by requiring opt-in consent for the processing of "sensitive data," permitting appeal of decisions by companies to deny consumer requests, as well as by imposing certain GDPR-style obligations such as the requirement to conduct data protection assessments. Because many of the privacy rights and obligations in the CPA are similar to those in the GDPR, CCPA, CPRA, and/or VCDPA, companies should be able to strategically leverage many of their existing or in-progress compliance efforts to ease their compliance burden under the CPA.

In light of this sweeping new law, we will continue to monitor developments, and are available to discuss these issues as applied to your particular business.

---

[1] Sec. 7(1), Colorado Privacy Act, Senate Bill 21-190, 73d Leg., 2021 Regular Sess. (Colo. 2021), to be codified in Colo. Rev. Stat. ("C.R.S.") Title 6.

[2] *E.g.*,C.R.S. §§ 6-1-1311(1); 6-1-108(1).

[3] SB 21-190 Signing Statement, *available at* https://drive.google.com/file/d/1GaxgDH_sgwTETfcLAFK9EExPa1TeLxse/view.

[4] C.R.S. § 6-1-1304(1).

[5] C.R.S. § 6-1-1304(2)(*l*).

[6] C.R.S. § 6-1-1304(2)(m).

[7] C.R.S. § 6-1-1304(2)(k), (n), (o).

[8] *E.g.*, C.R.S. §§ 6-1-1304(2)(e), (i)(II), (j)(IV), (q).

[9] C.R.S. § 6-1-1304(3)(a).

[10] C.R.S. § 6-1-1303(17).

[11] C.R.S. § 6-1-1303(17)(b).

[12] C.R.S. § 601-1304(2)(k).

[13] C.R.S. § 6-1-1303(24).

[14] C.R.S. § 6-1-1303(6)(a).

[15] C.R.S. § 6-1-1303(6)(b).

[16] C.R.S. § 6-1-1306(1)(b)-(e).

[17] C.R.S. § 6-1-1308(1)(a).

[18] C.R.S. § 6-1-1308(1)(a).

[19] C.R.S. § 6-1-1306(1).

[20] C.R.S. §§ 6-1-1306(1); 6-1-1308(1)(c)(I).

[21] C.R.S. § 6-1-1308(1)(c)(II), (6).

[22] C.R.S. § 6-1-1308(1)(d).

[23] C.R.S. § 6-1-1306(1)(a)(I).

[24] C.R.S. § 6-1-1303(23)(a) (emphasis added).

[25] C.R.S. § 6-1-1303(23)(b).

[26] C.R.S. § 6-1-1308(1)(b); *see also* 6-1-1306(1)(a)(III), 6-1-1306(1)(a)(IV)(C).

[27] C.R.S. § 6-1-1306(1)(a)(III).

[28] C.R.S. § 6-1-1306(1)(a)(II).

[29] C.R.S. § 6-1-1306((1)(a)(IV).

[30] C.R.S. § 6-1-1306((1)(a)(IV)(B).

[31] C.R.S. § 6-1-1303(24).

[32] C.R.S. § 6-1-1303(5).

[33] C.R.S. § 6-1-1303(5), (9).

[34] C.R.S. § 6-1-1306(2)(a)-(b).

[35] C.R.S. § 6-1-1306(2)(c).

[36] C.R.S. § 6-1-1306(3)(a).

[37] C.R.S. § 6-1-1306(3)(a)-(b).

[38] C.R.S. § 6-1-1306(3)(b)-(c).

[39] *See generally* C.R.S. §§ 6-1-1305, 6-1-1308(2)-(5).

[40] C.R.S. § 6-1-1308(2)-(4).

[41] C.R.S. § 6-1-1308(4).

[42] C.R.S. §§ 6-1-1305(3)(a); 6-1-1308(5).

[43] C.R.S. § 6-1-1309.

[44] C.R.S. § 6-1-1309(4).

[45] C.R.S. § 6-1-1305(3)-(5).

[46] C.R.S. §§ 6-1-1311(1)(a), (d).

[47] C.R.S. §§ 6-1-1311(1)(b); 6-1-1312.

[48] C.R.S. § 6-1-1311(1)(c); *see* C.R.S. § 6-1-112(a).

[49] C.R.S. § 6-1-1313(3).

This alert was prepared by Ryan Bergsieker, Sarah Erickson, Lisa Zivkovic, and Eric Hornbeck.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity and Data Innovation practice group.

Privacy, Cybersecurity and Data Innovation Group:

United States

Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Robert K. Hur – Washington, D.C. (+1 202-887-3674, rhur@gibsondunn.com)
Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)

Europe

Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0) 20 7071 4203, swazen@gibsondunn.com)

Asia

Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)