Cybersecurity, Privacy & Data Protection

Akin Gump
STRAUSS HAUER & FELD LLP

Colorado Privacy Act: What Businesses Need to Know

July 23, 2021

With the passage of the Colorado Privacy Act (CPA) during its latest legislative session, Colorado has become the third state to enact a comprehensive consumer data privacy law, following California and Virginia. Corporations that do business in Colorado will have two years to evaluate their data privacy practices and ensure they are prepared to comply with the CPA, which goes into effect on July 1, 2023.

Although the CPA does not feature groundbreaking privacy obligations, certain provisions do stand out. For instance, the law does not impose a revenue threshold, thus potentially subjecting small businesses who collect or profit from large amounts of personal data to comprehensive privacy obligations. Unlike the Virginia Consumer Data Protection Act (VCDPA), the CPA does not exempt nonprofits, nor does it expressly provide an entity-level exemption for organizations regulated by the Health Information Portability and Accountability Act (HIPAA).[1] Rather, like the California Consumer Privacy Act (CCPA), the CPA provides a data-based exemption by exempting certain HIPAA-regulated data from CPA regulation.[2] Further, the definition of “sell” is similar to that of the broad definition of “sell” in the CCPA, with the Colorado Attorney General (AG) set to establish technical specifications for a sale opt-out by July 1, 2023. Below we provide a primer on the key provisions of the CPA, including notable provisions that set the CPA apart from these predecessor statutes.

Who Must Comply with the CPA?

The CPA applies primarily to “controllers” and “processors,” both terms that appear prominently in the General Data Protection Regulation (GDPR). Under the CPA, a controller is “a person that, alone or jointly with others, determines the purposes for and means of processing personal data,”[3] and a “processor” is the “person that processes personal data on behalf of a controller.”[4] 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 the residents of Colorado,” and that satisfies one or both of the following thresholds:

- (a) controls or processes the personal data of 100,000 or more Colorado residents in a year; or

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Molly E. Whitman
Counsel
mwhitman@akingump.com
Los Angeles
+1 310.728.3737

Kelsey Stapler Morris
Counsel
kmorris@akingump.com
Irvine
+1 949.885.4226

Rachel Claire Kurzweil
Associate
rkurzweil@akingump.com
Washington, D.C.
+1 202.887.4253

Shelly A. Kim
Associate
shelly.kim@akingump.com
Los Angeles
+1 310.728.3333

- (b) both “derives revenue or receives a discount on the price of goods or services from the sale of personal data” and processes or controls the personal data of 25,000 or more consumers.[5]

While the CPRA only applies to businesses that derive annual gross revenue in excess of $25,000,000,[6] the Colorado statute does not impose such a revenue threshold. Consequently, the CPA may apply to more small, regional businesses than its California counterpart. As a practical matter, large, nationwide businesses that are subject to the CPRA, VCDPA or GDPR may already have many of the mechanisms in place required for compliance with the new Colorado law; in contrast, small and medium-sized businesses that may not have met the threshold requirements for these other statutes may be grappling with consumer data privacy requirements for the first time.

Which Entities—and What Data—is Exempt?

The CPA exempts certain entities and types of data from the law. But, notably, the CPA **does not** expressly exempt nonprofits or entities regulated by HIPAA from complying with the CPA. The law does provide for other entity-level exemptions such as air carriers, certain national securities associations and financial institutions subject to the Gramm-Leach-Bliley Act.[7]

The CPA also exempts certain types of data subject to state and federal laws, including protected health information that is collected, stored and processed by a covered entity or business associate, certain patient identifying information, information that is de-identified in accordance with the requirements for de-identification under HIPAA, the Fair Credit Reporting Act, the Gramm-Leach Bliley Act, the Driver’s Privacy Protection Act, the Children’s Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act.[8] If a controller processes personal data exempted from the CPA, the controller bears the burden of demonstrating that the processing qualifies for the exemption.[9]

What is “Personal Data” Under the CPA?

The CPA imposes obligations on companies to protect the privacy of consumers’ “personal data.” Personal data is defined under the CPA as “information that is linked or reasonably linkable to an identified or identifiable individual.”[10] It does not include employment data, de-identified or publicly available data. Covered businesses may only collect and use personal data for specific purposes, and must establish and maintain reasonable data security practices to protect the confidentiality, integrity and accessibility of personal data.[11]

Similar to the GDPR, CPRA and VCDPA, the CPA also regulates “sensitive data.” Sensitive data is defined under the Act as 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; genetic or biometric data; or personal data from a known child. As discussed further in this article, the CPA places more stringent requirements on the collection, processing and protection of consumers’ sensitive data than those required for personal data.

What Rights Do Colorado Consumers Have?

Not all Colorado residents are granted rights under the CPA: the law expressly exempts individuals acting in the commercial or employment context, including job applicants. This is different from the CPRA, where employees and job applicants are granted complete rights under the CPRA once the current exemption expires in 2023.

The CPA does grant similar consumer rights as under the California and Virginia privacy laws, including five key privacy rights: (1) the right to opt out of any processing for purposes of targeted advertising, sale to third parties,[12] or profiling in connection with decisions that produce legal or similarly significant effects; (2) the right to access their personal data; (3) the right to correct inaccuracies in their personal data; (4) the right to request that businesses delete their personal data; and (5) the right to obtain a portable copy of their personal data.[13]

The CPA also instructs the Colorado AG to establish regulations by July 1, 2023 that specify requirements for "one or more universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out" of ad targeting or sale of personal data.[14] Further, as of July 1, 2024, controllers must allow consumers to use such a "user-selected universal opt-out mechanism" that the AG has specified.[15] Notably, this requirement for a universal opt-out mechanism is similar to the requirement identified in the CCPA Regulations that businesses that collect personal information from consumers online treat Global Privacy Controls (GPC) as a valid request to opt-out of the sale of their personal information.[16] The California AG recently reaffirmed the requirement for businesses to honor GPCs in its updated CCPA FAQs and has sent notices companies subject to the CCPA for not honoring GPC signals.

What Constitutes Consent?

The CPA specifies that consumer consent to data processing may not be given via: (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;" or (c) "agreement obtained through dark patterns."[17] Rather, consumer consent must be provided by a "clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement," such as a written statement or some other clear, affirmative action.[18]

As with the CPRA, the CPA defines "dark pattern" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice."[19]

The concept of "dark pattern" behavior, which we discussed in a prior client alert, was highlighted recently in the Deceptive Experiences To Online Users Reduction (DETOUR) Act, proposed in the U.S. Senate in 2019. The Act, which was based on theories of behavioral economics, proposed to make it unlawful for large online operators to establish online interfaces in websites or apps that are designed to manipulate users into consenting to providing their data. It remains to be seen how authorities including the Colorado AG will interpret this concept.

What Obligations Do Controllers and Processors Have?

Similar to the obligations delineated in the VCDPA, the CPA places the following obligations on controllers:

- **Duties of transparency and purpose specification**: A controller must provide a reasonably accessible, clear and meaningful privacy notice to consumers that includes, among other things: (1) the categories of personal data collected or processed by the controller or a processor; (2) purposes for which personal data is processed; (3) how and where to exercise a consumer's individual rights; (4) the categories of personal data shared with third parties; (5) the categories of third parties with whom the controller shares personal data; and (6) the express purposes for which personal data is processed.[20]
- **Duty of 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 is processed.[21]
- **Duty to avoid secondary use**: A controller may not process personal data for purposes "that are not reasonably necessary or compatible with the specified purposes which the personal data are processed, unless the controller first obtains the consumer's consent."[22]
- **Duty of care**: A controller must take "reasonable measures to secure personal data during both storage and use from unauthorized acquisition," and those measures must "be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business."[23]
- **Duty to avoid unlawful discrimination**: A controller cannot process personal data in violation of state or federal laws prohibiting unlawful discrimination against consumers.[24]
- **Duty regarding sensitive data**: Like the VCDPA, the CPA requires a controller to obtain consumers' opt-in consent to process their sensitive data. When processing personal data concerning a known child, a controller must obtain consent from the child's parent or lawful guardian.[25] But unlike the VCDPA[26], the CPA does not expressly require compliance with the "verifiable parental consent" requirements of the COPPA.
- **Duty to conduct and document data protection assessment**: Like the VCDPA and CPRA, the CPA requires a controller to conduct and document data protection assessments before conducting processing that presents a "heightened risk of harm to a consumer."[27] Such scenarios include the processing of personal data for targeted advertising, certain profiling, selling personal data and processing sensitive data. The statute also provides the Colorado AG the right to request copies of a controller's data protection assessment.[28]

Similar to the GDPR, VCDPA and CPRA, the CPA also places several obligations on processors, including, among others: (1) to have processing activities be governed by a data processing agreement that sets forth the controller's processing instructions and specified obligations; (2) to take "appropriate technical and organizational measures" to assist the controller in responding to consumer's requests to exercise their rights; (3) to help the controller meet its obligations in relation to the security of processing and "in relation to the notification of a breach of the security system"; (4) to provide the controller with information necessary to "enable the controller to conduct and document data protection assessments"; (5) to "ensure that each person processing the personal data is subject to a duty of confidentiality"; and (6) to provide the controller with an opportunity to object to any subcontractor, and may only engage a subcontractor pursuant to a written agreement.[29]

Who Enforces the CPA?

Unlike the CPRA, the CPA does not grant consumers a private right of action for data breaches or any other violations.[30] Instead, only the Colorado AG and district attorneys are authorized enforce the CPA.[31] Prior to initiating any enforcement action, the AG or district attorney must issue a notice of violation to the controller and give the controller 60 days to cure the alleged violation, which doubles the 30-day cure period provided by the CPRA and VCDPA. However, this cure provision will sunset on January 1, 2025.[32]

The CPA also provides the AG with broad authority to promulgate rules "for the purpose" of carrying out the CPA. Further, the AG has discretion to adopt rules governing a process of issuing opinion letters and interpretive guidance to develop a framework for businesses that includes a good faith reliance defense of an action that may otherwise constitute a violation of the CPA. Such rules must be adopted by January 1, 2025.[33]

Key Takeaways

Although the CPA does not take effect until July 1, 2023, businesses should act now to determine their compliance obligations, including by performing a comprehensive data inventory, reviewing and updating internal policies, and reviewing their contracts with vendors and other service providers. Businesses should also update their public-facing privacy policies to, among other things, "clearly and conspicuously disclose the sale or processing" of personal data as well as the opt-out mechanism. But companies should also be on the lookout for legislative changes and interpretive regulations to come—in fact, shortly after Governor Jared Polis signed the CPA into law, he sent a letter to the Colorado General Assembly previewing future reform, stating that the law "will require clean-up legislation next year, and in fact, the sponsors, proponents, industry, and consumers are already engaged in conversations to craft that bill." In the meantime, companies subject to the CPA along with the California and/or Virginia laws, both of which go into effect on January 1, 2023, should coordinate their compliance efforts to ensure a streamlined and efficient transition to compliance with these laws.

[1] The VCDPA explicitly exempts nonprofit organizations, and covered entities and business associates subject to HIPAA, "[t]his chapter shall not apply to any… (iii) covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5); (iv) nonprofit organization…" VCDPA, § 59.1-572(B).

[2] *See* Cal. Civ. Code § 1798.145(c).

[3] S.B. 21-190 § 6-1-1303(7).

[4] *Id.* § 6-1-1303(19).

[5] *Id.* §§ 6-1-1303(6); 6-1-1304(1).

[6] Cal. Civ. Code § 1798.140(c) (The CPRA applies to businesses that conduct business in California and satisfies one or more of the following thresholds: (1) Has annual gross revenue in excess of $25,000,000; (2) annually buys, receives, sells, or shares personal information of 50,000 or more consumers, households, or devices; or (3) derives 50% or more of its annual revenue from selling consumers' personal information.).

[7] *Id.* § 6-1-1304(2)(j).

[8] *Id.* § 6-1-1304(2)(l)-(m), (q).

[9] *Id.* § 6-1-1304(5).

[10] S.B. 21-190 § 6-1-1303(17)(a).

[11] *Id.* § 6-1-1308.

[12] Notably, “sale” is defined as “the exchange of personal data for monetary or other valuable consideration by a controller to a third party,” which models the CPRA’s definition of the term. *Id.* § 6-1-1303(23)(a).

[13] *Id.* § 6-1-1306.

[14] *Id.* § 6-1-1313.

[15] *Id.* § 6-1-1306(1)(a)(IV)(B).

[16] 11 Cal. Code Regs. § 999.315(c).

[17] *Id.* § 6-1-1303(5)(a)-(c).

[18] *Id.* § 6-1-1303(5).

[19] *Id.* § 6-1-1303(9).

[20] *Id.* § 6-1-1308(1)-(2).

[21] *Id.* § 6-1-1308(3).

[22] *Id.* § 6-1-1308(4).

[23] *Id.* § 6-1-1308(5).

[24] *Id.* § 6-1-1308(6).

[25] *Id.* § 6-1-1308(7).

[26] VA Code Ann. § 59.1-572(D) (“Controllers and processors that comply with the verifiable parental consent requirements of the Children’s Online Privacy Protection Act (15 U.S.C. § 6051 *et seq*.) shall be deemed compliant with any obligation to obtain parental consent under this chapter.

[27] S.B. 21-190 § 6-1-1308(5).

[28] *Id.* § 6-1-1309.

[29] *Id.* § 6-1-1305.

[30] *Id.* § 6-1-1310.

[31] *Id.* § 6-1-1311.

[32] *Id.* § 6-1-1311(1)(d).

[33] *Id.* § 6-1-1313(3)

akingump.com