ALERT MEMORANDUM

The Centennial State Claims a New Number: Colorado to Become Third State in the U.S. to Enact Comprehensive "Privacy Act"

July 1, 2021

Colorado is set to become the third state in the nation to enact comprehensive privacy legislation with the passing of SB 21-190, more commonly known as the Colorado Privacy Act ("ColoPA" or the "Act"). Governor Jared Polis is expected to sign the ColoPA into law in the coming days, after which the Act will become effective July 1, 2023, giving covered entities roughly two years to become compliant.

While the ColoPA draws heavily from Virginia's Consumer Data Protection Act ("VDPA"), the California Privacy Rights Act of 2020 ("CPRA"), which amends and expands the California's Consumer Privacy Act ("CCPA"), and the European Union's General Data Protection Regulation ("GDPR"), there are material differences amongst these laws. Without federal legislation that includes preemption, it is likely that states will continue to enact privacy laws and that such laws will continue to diverge from one another in nuanced ways. To combat rising compliance costs and growing uncertainty for covered entities, commissioners at the Federal Trade Commission have begun to discuss using their rulemaking authority to establish a unified privacy framework. Until that time, however, covered entities must remain informed of their obligations under each law applicable to them and adapt their privacy programs accordingly.

Below we summarize key elements of the Act while highlighting its similarities and differences with the CCPA/CPRA, VDPA and GDPR. [1]

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

NEW YORK

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

Jonathan Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Megan Medeiros
+1 212 225 2072
mmedeiros@cgsh.com

Melissa Faragasso
+1 212 225 2115
mfaragasso@cgsh.com

[1] The full text of the Colorado Privacy Act is available here.

Who must comply?

- Beginning July 1, 2023, the ColoPA will apply to legal entities that conduct business or produce or deliver commercial products or services that are intentionally targeted to Colorado residents that *either*: (i) control or process the personal data of more than 100,000 consumers[2] per calendar year; or (ii) derive revenue from the sale of personal data and control or process the personal data of at least 25,000 consumers. Like the VDPA, the ColoPA's threshold for applicability is geographically targeted, meaning an entity must collect data from a large number of Colorado consumers (whether 100,000 or 25,000 consumers) to be covered by the Act, whereas an entity can be covered by the CCPA if it has a global annual revenue of $25,000,000 and does business in California regardless of the number of California residents affected (as long as it collects personal data of one or more California residents).

- In line with the CCPA and VDPA, the Act provides a list of enumerated exceptions and does not apply to de-identified data[3], certain listed activities and categories of personal data[4], personal data governed by other listed state and federal laws[5] and personal data contained in employment records.

What data is protected?

Like the VDPA and CPRA, the ColoPA distinguishes between "personal data" and "sensitive data", and contains varying protections for each.

The ColoPA defines personal data as "information that is linked or reasonably linkable to an identified or identifiable individual; and does not include de-identified data or 'publically available information'[6]."

- Interestingly, the definition of personal data is not tied to "consumers", which arguably broadens certain obligations that reference "personal data" but not "consumers"

[2] Defined as "an individual who is a Colorado resident acting only in an individual or household context; and does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context."

[3] Defined as "data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual if the controller that processes the data:

(a) takes reasonable measures to ensure that the data cannot be associated with an individual;

(b) publicly commits to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data; and

(c) contractually obligates any recipients of the information to comply with the requirements of this subsection 11."

[4] Including protected health information, identifiable private information collected in connection with human subject research, patient identifying information maintained by certain substance abuse treatment facilities, and data maintained by air carriers, national securities associations, public utilities and state institutions of higher learning.

[5] Including healthcare entities and health-related data governed by the Health Insurance Portability and Accountability Act and information and personal data covered under the Fair Credit Reporting Act, the Gramm Leach Bliley Act, the Driver's Privacy Protection Act, the Children's Online Privacy Protection Act and the Family Educational Rights Act and Privacy Act

[6] Means "information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public."

specifically. For example, under ColoPA, controllers have, with respect to personal data, a duty of data minimization (discussed further below) which limits their data collection to what is reasonably necessary under the specified purposes for which the data are processed. A plain reading of this requirement suggests that controllers must practice data minimization in all instances of personal data collection. Arguably, this obligation could apply to the personal data of non-Colorado residents once the entity is subject to the ColoPA due to their initial processing of Colorado resident information. In contrast, the CCPA/CPRA clearly define personal information to mean information that identifies or could reasonably be linked, directly or indirectly, with a particular "consumer" (which is in turn defined as a California resident); thus, the statute makes clear that the rights of consumers, as well as the obligations and restrictions placed on covered entities, are specific to California residents.

- Another curious point to note, under the ColoPA, the definition of "consumer" covers Colorado residents acting in an individual *or household context*; however, "personal data" under the Act only covers information that is linked or reasonably linkable to an "individual", and not to an entire household. Thus, arguably, where data is collected that relates to a number of individuals within a household, but is not capable of being linked to one specific individual within that household, the rights afforded to Colorado consumers under the Act may not apply.[7]

ColoPA defines "sensitive data" as "personal data revealing racial or ethical 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 that may be processed for the purpose of uniquely identifying an individual or personal data from a known child."

- This definition is slightly narrower than the VDPA's and CPRA's definitions, both of which include precise geolocation data. Additionally, the CPRA's definition also includes financial information, government identifying information, such as driver's license, passport, and social security numbers, and the content of consumer's private communications such as emails or text messages.

The ColoPA places two obligations on covered entities with respect to sensitive data. First, data controllers may not process a consumer's sensitive data without first obtaining the consumer's affirmative, *GDPR-style consent*[8], or in the case of a child, without first obtaining a parent or guardian's consent. In other words, the ColoPA, somewhat like the VDPA[9], requires a specific opt-in approach before consumers' sensitive data is processed.

[7] Contrast with the CCPA where "household" is defined (in the CCPA Regulations) as "a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier".

[8] 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 Act also makes clear that consent cannot be obtained by way of acceptance of general or broad terms of use or through dark patterns, which is a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice.

[9] The VDPA requires consent prior to processing of sensitive data.

- Conversely, the CPRA, which amended the CCPA to distinguish between personal and sensitive data, does not require businesses to receive consumer consent prior to processing sensitive data. Instead, CPRA covered entities can use sensitive data so long as they (i) disclose to consumers the categories of sensitive data to be collected, the purposes for the collection and use of such data and whether the data is sold or shared and (ii) with respect to certain sensitive data that is collected or processed with the purpose of inferring characteristics about consumers (to be further defined in CPRA regulations), provide consumers with a right to limit the entity's use of the consumer's sensitive data to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer (i.e. a limited opt-out approach).

The second obligation ColoPA places on data controllers is to restrict controllers from processing sensitive data where such processing presents a heightened risk of harm to a consumer, without first conducting and documenting a data protection assessment for each of its processing activities. This requirement is discussed further below.

What obligations are placed on covered entities?

Drawing from the VDPA and the GDPR, the Act distinguishes between data controllers and data processors, and provides requirements for each with respect to the processing of personal data. Under the ColoPA, a data controller is defined as a person that, alone or jointly with others, determines the purposes and means of processing personal data. A data processor on the other hand refers to a person that processes personal data on behalf of a data controller.

Data controllers and processors must both adhere to provisions under ColoPA; however, data controllers have the primary responsibility for most of the Act's obligations. ColoPA imposes a variety of duties and obligations on controllers, including:

- *The Duty of Transparency*. Controllers must provide a reasonably accessible, clear and meaningful privacy notice detailing: (i) the categories of personal data collected and purposes for which the personal data is processed; (ii) how and where consumers can exercise their rights (including how to contact the controller or appeal a controller's action with regard to a consumer request); (iii) the categories of personal data that the controller shares with third parties, if any; (iv) the categories of third parties, if any, with whom the controller shares personal data; and (v) if the controller sells or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose such practices and how the consumer can opt out, as discussed further below;

- *The Duty of Purpose Specification*.

- *The Duty of Data Minimization*. Controller's activities must be "adequate, relevant and limited to what is reasonably necessary" in relation to the specified processing purposes;

- *The Duty to Avoid Secondary Use*. Absent consumer consent, Controllers are restricted from processing data inconsistently with the specified purposes for which the personal data is processed;

- *The Duty of Care*. Controllers must take reasonable measures to secure personal data during both storage and use;

- *The Duty to Avoid Unlawful Discrimination*; and

- *The Duty Regarding Sensitive Data.*

In addition, the Act requires:

Data Protection Assessments. Controllers are required to conduct data protection assessments for each of its processing activities that involve personal data and present a heightened risk of harm to consumers. Activities that present a heightened risk to consumers include (i) processing personal data for the purposes of targeted advertising or profiling, if the profiling presents a reasonably foreseeable risk of (a) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (b) financial or physical injury to consumers, (c) 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 (d) other substantial injury to consumers; (ii) selling personal data; or (iii) processing sensitive data.

- Like the VDPA, data protection assessments must identify and weigh the benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer, as mitigated by safeguards employed by the controller to reduce such risks. The data controller must also consider the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose data will be processed. Upon request, controllers must make these data protection assessments available to the Attorney General.

- While the CCPA does not currently require data protection assessments, under the CPRA amendments, businesses that process personal information that presents a significant risk to consumers' privacy or security must conduct risk assessments with respect to the processing of such personal information and submit the report to regulators. Notably, these requirements are similar to the VDPA's and GDPR's data protection impact assessment obligations.

Data Processing Agreements. Like Article 28 of the GDPR, before transferring or processing data ColoPA requires controllers and processors to enter into data processing agreements containing (i) processing instructions, including the nature and the purpose of the processing; (ii) the type of personal data subject to the processing and the duration of such processing; (iii) a requirement to delete or return personal data, upon request, to the controller at the end of the provision of services; and (iv) audit and inspection rights.

Finally, the Act places additional specific obligations on data processors including requirements to (i) implement measures to assist with controllers' responses to consumer rights requests; (ii) help controllers meet their security and breach notification obligations; (iii) ensure individual processing data are subject to a duty of confidentiality; and (iv) engage with subcontractors, subject to controller consent, pursuant to a written contract requiring the subcontractor to meet all of the processor's obligations.

What rights do Colorado consumers have under the Act?

The ColoPA provides the following rights to Colorado "consumers"

- *Access Rights*. The right to confirm whether a controller is processing the consumer's personal data and to access such personal data;

- *Correction Rights*. The right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

- *Deletion Rights*. The right to have personal data provided by or obtained about the consumer deleted;

- *Data Portability Rights*. The right to obtain a copy of the consumer's personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance; and

- *Opt Out Rights*. The right to opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

    - Unlike the CCPA or VDPA, a controller may provide a user-selected universal opt-out mechanism for consumers to exercise the right to opt-out; however effective July 1, 2024, controllers *must* allow consumers to exercise their opt-out right through a user-selected universal opt-out mechanism that meets the technical specifications established by the Attorney General. The ColoPA provides the Attorney General rulemaking authority and requires the adoption of detailed rules outlining the technical specifications for this universal opt-out mechanism by July 1, 2013.

    - The ColoPA definition of sale aligns more closely with the CCPA/CPRA, as opposed to the VDPA and Nevada's online privacy notice statutes. ColoPA defines sale as "the exchange of personal data for monetary or other *valuable* consideration by a controller to third party" but does not include disclosures to (i) data processors, defined above, (ii) a third party for purposes of providing a product or service requested by the consumer; (iii) controller affiliates; (iv) to a third party of personal data as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets; or (v) (a) that a consumer directs the controller to disclose or intentionally discloses by using the controller to interact with a third party; or (b) intentionally made available by a consumer to the general public via a channel of mass media. The VDPA and Nevada's online privacy notice statutes, define sale to only cover transfers of personal data for *monetary* consideration.

It is important to note that the consumer rights above do not apply to "pseudonymous data"[10] if the controller can demonstrate that the information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

No private right of action - what are the penalties for non-compliance?

Similarly to the VDPA, and contrary to the CCPA (with respect to a violation of the duty to implement and maintain reasonable security procedures and practices), the ColoPA does not contain a private right of action for individuals, and subjects the violating entity to penalty amounts of up to $2,000 per violation with a maximum of $500,000 for related violations. Furthermore, a violation of the Act is considered a deceptive trade practice as defined under Colorado Revised Statutes, 6-1-105.

Upon notice, violators are provided 60 days to cure[11] before an action may be brought; however, effective January 1, 2025, the Act will no longer provide a cure period for alleged violations, making violations of the Act immediately actionable.

The Changing Legal Landscape

While the possibility of federal legislation hangs in the balance, states have and will continue to introduce their own privacy bills across the country, further complicating covered entities' ability to ensure compliance across state lines. Luckily, as noted above, we are seeing significant overlap between the existing state privacy laws and those coming into effect in the coming years, though such consistency is not guaranteed in future state legislation. In any event, covered entities should begin working towards implementing new data principles and mechanisms that are likely to be present in future laws, such as data minimization and privacy by design, not only to ensure legal compliance, but also to remain competitive and retain their consumers' trust. This includes evaluating and reconfiguring internal practices and policies with an eye toward understanding what data the entity collects, how and for what purposes it is used and processed, with whom it is shared and how to ensure appropriate safeguards to protect the data and minimize risks to consumers.

…

CLEARY GOTTLIEB

[10] Defined as "personal data that can no longer be attributed to a specific individual without the use of additional information if the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to a specific individual".
[11] Note that this cure period exceeds VDPA and CCPA cure periods, which only last 30 days.