HUSCH BLACKWELL

COLORADO PRIVACY ACT RESOURCE CENTE

On July 7, 2021, Colorado officially became the third state – after California and Virginia – to pass broad consumer privacy legislation when Governor Jared Polis signed the Colorado Privacy Act (CPA) into law. The CPA went into effect on July 1, 2023.

To assist companies in understanding and complying with the CPA, Husch Blackwell's Denver-based data privacy team has compiled numerous resources and FAQs.

FREQUENTLY ASKED QUESTIONS

What businesses does the Colorado Privacy Act apply to?

The Colorado Privacy Act applies to "controllers" that conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to Colorado residents and that either (1) control or process the personal data of 100,000 or more consumers during a calendar year or (2) derive revenue or receive a discount on the price of goods or services from the sale of personal data and process or control the personal data of 25,000 or more consumers.

The law defines "consumers" to mean Colorado residents acting only in an individual or household context. It does not include Colorado residents acting in a commercial or employment context.

When determining whether the law applies, businesses should note that the CPA does not have a monetary threshold for applicability similar to the California

Contact Information

David M. Stauss
303.892.4429
david.stauss@
huschblackwell.com

Consumer Privacy Act's (CCPA) $25,000,000 annual gross revenue threshold. Further, the law's 100,000/25,000 consumer thresholds apply to personal data that is either controlled or processed. The CPA defines "process" to include not only data collection, but also its storage. In other words, businesses need to be mindful of counting the data that they currently store, not just what they collect on an annual basis.

How does the Colorado Privacy Act define personal data?

Personal data is defined as "information that is linked or reasonably linkable to an identified or identifiable individual." It does not include de-identified data or publicly available information.

Does the Colorado Privacy Act exempt any types of businesses?

Yes. The law does not apply to certain types of entities and data sets, such as financial institutions subject to the Gramm-Leach-Bliley Act, many types of healthcare-related data and data governed by FERPA. Businesses that are already subject to federal privacy laws should review the law's exemptions to see if any apply.

Does the Colorado Privacy Act apply to nonprofits?

Yes. In a significant change from the California and Virginia laws, the Colorado Privacy Act does not exclude nonprofits.

What rights does the Colorado Privacy Act provide to Colorado residents?

The Colorado Privacy Act provides Colorado residents with the right to opt out of targeted advertising, the sale of their personal data, and certain types of profiling.

Starting July 1, 2024, controllers will need to honor user-selected universal opt-outs for targeted advertising and sales. Colorado residents also have the rights to access, correct, and delete their personal data as well as the right to data portability. Controllers will generally have 45 days to respond to consumer requests.

How does the Colorado Privacy Act define the "sale" of personal data?

"Sale" is defined as "the exchange of personal data for monetary or other valuable consideration by a controller to a third party." The definition contains certain exceptions such as the disclosure of personal data to a processor that processes the personal data on behalf of a controller and the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer.

How does the Colorado Privacy Act define targeted advertising?

Targeted advertising means displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests. It does not include advertising to a consumer in response to the consumer's request for information or feedback; advertisements based on activities within a controller's own websites or online applications; advertisements based on the context of a consumer's current search query, visit to a website, or online application; or processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

How does the Colorado Privacy Act define profiling?

Profiling means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Does the Colorado Privacy Act require businesses to have online privacy policies?

Yes. Controllers need to provide a "reasonably accessible, clear, and meaningful privacy notice" that identifies information such as the categories of personal data that are collected or processed, the purposes for which the data are processed, how consumers can exercise their rights, and disclosures around the selling and sharing of personal data.

Does the Colorado Privacy Act require that a business obtain consent for the collection of personal data?

Yes, for certain types of information. Specifically, controllers must obtain consumer consent prior to processing sensitive data. The law defines sensitive data to include personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, citizenship or citizenship status, genetic or biometric data that may be processed for the purpose of uniquely identifying an individual, and the personal data of a known child.

Does the Colorado Privacy Act restrict data collection?

Yes. The Colorado Privacy Act requires controllers to (1) specify the express purpose for which personal data are collected and processed (duty of purpose specification); (2) restrict their data collection to data that is "adequate, relevant and limited to what is reasonably necessary in

relation to the specified purposes for which the data are processed" (duty of data minimization); (3) not process personal data for purposes that are not reasonably necessary or compatible with the specified purposes for which the data were collected without consumer consent (duty to avoid secondary use); and (4) properly secure personal data (duty of care).

Does the Colorado Privacy Act require businesses to enter into data processing agreements with processors?

Yes, the Colorado Privacy Act requires controllers to enter into data processing agreements (DPAs) with processers. Among other things, DPAs must (1) contain processing instructions, including the nature and purpose of the processing; (2) identify the type(s) of personal data that will be processed; (3) bind processors and their employees to confidentiality; (4) require processors to implement appropriate security measures to protect personal data; (5) address the return or deletion of personal data; (6) require processors to allow for audits; and (6) require processors to enter into similar contracts with sub-processors.

Does the Colorado Privacy Act require businesses to conduct data protection assessments?

Yes. Prior to engaging in processing that presents a heightened risk of harm to consumers, controllers must conduct and document data protection assessments. This includes processing personal data for targeted advertising or sales, certain types of profiling, and processing sensitive data.

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 consumers associated with the processing.

The Colorado Attorney General can request data protection assessments; however, such a request does not constitute a waiver of the attorney client privilege or work product protection (thereby implying that assessments can be so protected).

How is the Colorado Privacy Act enforced?

The Attorney General and district attorneys have exclusive authority to enforce the CPA and can seek injunctive relief or significant monetary damages. There is no private right of action.

Initially, the CPA requires the Attorney General or district attorneys to issue a notice of violation and allow entities 60 days to cure the alleged violation – i.e., a right to cure. The right to cure will sunset on January 1, 2025. In lieu of a right to cure, controllers will be able to request opinion letters and interpretative guidance from the Attorney General's office.

When did the Colorado Privacy Act go into effect?

The Colorado Privacy Act went into effect on July 1, 2023.

What other Colorado privacy and data security laws should I be aware of?

Colorado has a number of other statutes that entities should consider when complying with the Colorado Privacy Act. The below statutes apply to certain types of entities that are not covered by the Colorado Privacy Act. Therefore, entities that may not be subject to the Colorado Privacy Act, should still review these laws to see whether compliance is required.

Colorado's Information Security Law

Colorado's information security law, C.R.S. § 6-1-713.5, requires covered entities that maintain, own, or license personally identifiable information of Colorado residents to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personally identifiable information and the nature and size of the business and its operations." If a covered entity contracts with a third-party service provider to maintain, store, or process personally identifiable information, the covered entity must require that the third-party service provider implement and maintain reasonable security procedures and practices.

The law defined "personally identifiable information" as a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data; an employer, student or military identification number; or a financial transaction device.

The law does not define what constitutes reasonable security measures.

This statute should be read in conjunction with the Colorado Privacy Act's requirement that controllers must enter into data processing agreements with processors that govern the processing of personal data. Whereas the Colorado Privacy Act only applies to certain types of entities, Colorado's information security law applies more broadly. Accordingly, entities that are not subject to the Colorado Privacy Act still may be required to contractually ensure that third party service providers implement reasonable security procedures when handling certain types of data. Similarly, both laws require that entities implement reasonable security procedures to protect personal data / personally

identifiable information.

Colorado's Document Disposal Law

Colorado's document disposal law, C.R.S. § 6-1-713, requires public and private entities to develop a policy for the destruction or proper disposal of paper documents containing personally identifiable information.

Colorado's Data Breach Notification Law

Colorado's data breach notification law, C.R.S. § 6-1-716, requires "covered entities" to notify affected individuals and other entities if they experience a security breach. The law defines "covered entity" as a person (as defined C.R.S. § 6-1-102(6)) that maintains, owns, or licenses personal information in the course of the person's business, vocation, or occupation. Notably, the definition of "covered entity" is broader than the Colorado Privacy Act's definition of "controller."

"Security breach" is defined as the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.

"Personal information" is broadly recognized as a Colorado resident's first name or first initial and last name in combination with any of the following data elements:

Social security number;

Student, military, or passport identification number;

Driver's license number or identification card number;

Medical information;

Health insurance identification number; or

Biometric data

Personal information also includes a Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account, and a Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.

Unless an exception applies, covered entities have 30 days to notify affected individuals and provide certain information as required by the statute. If the covered entity notifies 500 or more Colorado residents, it also must notify the Colorado Attorney General's office.

The law contains a safe harbor provision for covered entities that develop and comply with their own notification procedures that are consistent with the law's requirements. To take advantage of that provision, covered entities should consider developing and implementing an incident response plan as part of their Colorado Privacy Act compliance.

The statute has additional requirements and exceptions not discussed here. Any entity that believes it may have a reporting obligation should consult the statute and the Colorado Attorney General's FAQs.