September 15, 2021

Colorado Privacy Act: Another Piece to the Data Privacy Puzzle

Mir Ali, Elana Egri-Thomas

Ankura Cybersecurity & Data Privacy

[co-author: Aidan Morrissey]*

Introduction

Privacy laws have entered the compliance world by storm and are quickly changing data privacy practices. The most recent state, Colorado, passed the Colorado Privacy Act (CPA) into law on July 7, 2021. This new act follows California's Consumer Privacy Act (CCPA) but calls out several additional rights, actions, and policies. The CPA pulls certain consumers rights and practices from the EU's General Data Protection Regulation (GDPR). One may observe that the CPA is a hybrid of the CCPA and GDPR.

Key Components

Privacy Impact Assessments

The new Colorado Privacy Act requires privacy impact assessments. Very similar to the GDPR, these impact assessments are intended to aid companies in identifying risk to consumers. In addition, the CPA identifies the need to assign controllers and processors which is another resemblance to the GDPR. The act states that "data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer". To be prepared to create privacy impact assessments, companies should also focus on creating a comprehensive data inventory – a requirement which, although isn't explicitly stated in all privacy regulations, is a necessary foundation component of a mature data privacy program.

Consumers Rights

Consumer rights are one of the many similarities of both the CCPA and the GDPR. The act identifies and establishes certain rights for consumers as outlined below:

- **Right of Access -** The right of access provides a consumer with the right to access any information that a specific entity may hold. The consumer "has the right to confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data".

- **Right of Correction** - Also known as the right of rectification, this aspect allows Colorado consumers to have their information corrected or ratified. The consumer "has the right to correct inaccuracies in the consumer's personal data".

- **Right of Deletion -** The right of deletion allows consumers to have an entity delete any personal information about them. The law does recognize certain restrictions on this process and outlines the legal practices of retaining certain personal information regardless of the consumer's request. The consumer "has the right to delete personal data concerning the consumer".

- **Right of Portability -** The rights included in portability give the consumer control and ownership of their data. The entity has the obligation to provide requested information in a readily accessible format. With this right, the consumer may reuse their data in an efficient and effective manner.

- **Responding to Consumer Requests -** The act states that requests are to be completed "without undue delay and, in any event, within forty-five days after receipt of the request". The act also outlines all responsibilities of the processor to complete the request.

Exemptions

Current exemptions may apply for personal data held by a controller. See below for how the CPA defines those exemptions. It's important to note that data maintained for employment purposes is currently out of scope for the CPA. This is a similarity to the CCPA, however, in 2023 the new iteration of the CCPA, called the CPRA, will come into play and this new iteration will apply to employees. It will be interesting to see if states continue to exclude employee data, or if the U.S. will follow in Europe's footsteps and include employee data for data protection purposes.:

- Data maintained for employment purposes

- Children's data regulated by the Children's Online Privacy Protection Act of 1998

- A National Securities Association registered entity

- Customer data maintained by a public utility

- Data maintained by state institution of higher education
- A financial institution subject to GLBA
- Anything that restricts a controllers ability to
    - Comply with civil, criminal, or any investigation
    - Cooperate with law enforcement

Sensitive Data

Sensitive data is identified as “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…c) personal data from a known child”. The controller has a duty to receive a consumer’s consent to process sensitive data. Much like the GDPR, if sensitive data is to be collected, clear consent must be given outside of just accepting terms and conditions.

Right to Opt-out

The act states that “the right to opt out not only of the sale of personal data but also of the collection and use of personal data”. In general, opting out is a term used to give consumers the right to revoke permission of personal data use. The CPA identifies and outlines the exact rights of each consumer. These rights include “the right to opt-out of the processing of personal data concerning the consumer for purposes of: targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer”.

Duty of Transparency

The duty of transparency provides consumers with the right to a privacy notice and data breach notifications. The privacy notice should include the categories of personal data, the purpose of processing activities, how consumers may execute their rights, and categories of personal data shared with third-party vendors. This requirement is very similar to the California privacy notice which also requires categories of information collected and shared to be explicitly stated.

Enforcement

There is no private right of action; the attorney general will act on behalf of any complaint. The CPA may follow a CCPA style enforcement of holding minimum fines and using punitive damages

to further aid privacy law enforcement.

Looking Ahead

This act provides consumers with the rights to take control of their data and gives the right to understand how their data is processed. As we look forward to a more secure data driven industry, Colorado will lead alongside California as a prominent role model by showcasing a consumer-focused privacy law.

[1]The information provided in this article is for general informational purposes only and does not, and is not intended to, constitute legal advice.

**Intern*

RELATED POSTS

- Overview of California AG's Examples of CCPA Non-Compliance
- Lessons Learned from Implementing Privacy Rights Request Processes – Part 1
- Implementing the NIST Privacy Framework – Identify Function
- Hidden tips related to "Do Not Sell" in the CA AG's Online Consumer Privacy Tool

LATEST POSTS

- Overview of California AG's Examples of CCPA Non-Compliance

See more »

WRITTEN BY:

Ankura Cybersecurity & Data Privacy

Contact + Follow

Mir Ali + Follow

 Elana Egri-Thomas + Follow

PUBLISHED IN:

California Consumer Privacy Act (CCPA) + Follow

California Privacy Rights Act (CPRA) + Follow

Colorado + Follow

Enforcement Actions + Follow

General Data Protection Regulation (GDPR) + Follow

Impact Assessments + Follow

Opt-Outs + Follow

Personal Data + Follow

Popular + Follow

Right of Access + Follow

Sensitive Personal Information + Follow

State Privacy Laws + Follow

more

ANKURA CYBERSECURITY & DATA PRIVACY ON: