CLIENT ALERTS & INSIGHTS

New Colorado Privacy Act Regulations Advance, Putting in Place Consent Requirements for Those Under the Age of 18

DECEMBER 18, 2024

The Colorado Department of Law adopted new regulations governing the collection and use of biometric identifiers and information about those under the age of 18 and put in place a new mechanism through which businesses can seek guidance for proposed data processing activities. In early December, the Colorado Department of Law adopted a slate of new regulations under the Colorado Privacy Act. The new regulations, once published, will take effect within 30 days-which will occur after the Colorado Attorney General issues their formal opinion.

The new regulations focus on biometric identifiers and personal data about those under the age of 18. In June, the Colorado legislature passed amendments to the Colorado Privacy Act to include new biometric identifier requirements-which aligned closely to what existing biometric privacy laws require but stopped short of introducing a private right of action for violations or misuse of biometric identifiers. To see more coverage on the previous biometric identifier amendments, see here.

The new regulations also broaden what the Colorado Privacy Act considers to be a "minor" to anyone under the age of 18. Under the new regulations, express opt-in consent is required before processing the personal data of a consumer whom a business knows is a minor (i.e., under the age of 18) and before processing biometric identifiers in any manner.

The new regulations expand on and provide important context-while also imposing new requirements-to the existing Colorado Privacy Act. Additionally, the new regulations create a process through which the Colorado Attorney General's Office can issue opinion letters, providing businesses greater clarity on the Colorado Privacy Act's requirements.

The Colorado Privacy Act was among the first broad, omnibus data protection laws in the U.S. following California's foray via the California Consumer Privacy Act. The Colorado Privacy Act took effect in 2023. To see more on other U.S. state data protection laws, see Data Meets World's U.S. State Privacy Laws webpage.

See more details on the new regulations below.

Consent Requirements for Collection of Data From Minors

The Colorado Privacy Act already defined "sensitive personal data" to include personal data about a child, which matched federal law's definition of a child under the Child Online Privacy Protection Act-setting the age cut off to anyone under the age of 13. The Colorado Privacy Act requires that businesses obtain prior consent before processing sensitive personal data generally. For those

under the age of 13, consent would need to come from a parent or legal guardian-which tracks with federal law.

The new regulations introduce the newly defined term “Minor,” which means any person under the age of 18 years old.

Under the new regulations, businesses are required to obtain prior, opt-in consent before (1) processing the personal data of a person that the business actually knows is a minor or should have known but for willful disregard; and (2) using any system design feature that significantly increases, sustains or extends the use of services or features by a person that the business actually knows is a minor or should have known but for willful disregard.

Earlier drafts of the regulations included a broader knowledge basis for the consent requirement, meaning any business that interacted with minors-whether they had actual knowledge of minors using their services or websites-would have had to take note. However, under the new proposed regulations, the consent requirement is tied to either active knowledge or willful disregard on the part of the business.

In addition to the prior consent requirements, the new regulations require in-scope businesses to conduct data protection assessments for features designed to increase, sustain, or extend the use of services by minors.

Biometric Identifiers

Tracking with Colorado’s previous amendments that included more robust biometric identifier consent and notice requirements, the new regulations require prior, opt-in consent for processing or using biometric identifiers in any manner.

“Biometric identifiers” are defined as data generated by technological processing, measurement, or analysis of a consumer’s biological, physical or behavioral characteristics. Examples of biometric identifiers include fingerprints, voiceprints, retina and iris scans, and facial geometry measurements or scans (e.g., facial recognition).

The new regulations also implement clear guidelines on the form of notice businesses need to make to consumers and employees when they collect biometric identifiers . This notice is required to occur at or before the time of collection and meet the Colorado Privacy Act’s general privacy notice requirements-such as providing information on the type of biometric identifiers collected, purposes the biometric identifiers are used for, who the biometric identifiers are disclosed to, and rights the consumer or employee may have with respect to the biometric identifiers.

The biometric identifier privacy notice requirements can be met through and included in a business’s general privacy notice-or, in the case of employee biometric identifiers, in the business’s general employee privacy notice.

Refreshing Consent

The existing Colorado Privacy Act regulations require businesses-who are subject to prior consent requirements such as the sensitive personal data prior opt-in consent requirements-to refresh consent with certain persons who already consented. Where a business has not interacted with a person in 24 months, consent must be obtained again.

For example, if a business initially collects information about a 15-year-old user, but has no subsequent interaction with that user for 24 months, they must again obtain prior express consent for a subsequent collection or use of data.

Where biometric identifiers are collected by employers from employees, the refreshed consent requirement allows for a bit more flexibility. In such circumstances, employers are only required to refresh consent to collect biometric identifiers from employees (1) when additional categories of biometric identifiers are collected; or (2) when biometric identifiers are used for a secondary purpose not specified in the initial consent / notice.

Opinion Letters

Under the new regulations, the Colorado Attorney General's Office will have discretion whether to issue opinion letters. The substance of opinion letters will aim to explain the application of provisions and requirements under the Colorado Privacy Act.

Businesses can request opinion letters, but the request must be (1) prospective in nature, pertaining to an activity that the requestor specifically plans to undertake; (2) must not be based on a hypothetical situation or activity not related to the requestor; and (3) must be in writing. The request for an opinion letter must then substantively contain the following:

- Complete and specific description of the activity and planned processing;
- Description of the personal data in scope, including whether sensitive personal data is in scope;
- Description of the parties who will have access to the personal data;
- Description and draft of any planned consumer-facing disclosures relating to the planned activity;
- A copy of any data protection assessment conducted in anticipation of the planned activity; and
- A designation of trade secrets or confidential information included, if applicable.

If the Colorado Attorney General's Office determines it will publish an opinion letter pursuant to the request, an opinion letter will be publicly issued, redacting and protecting designated information.

Conclusion

The new regulations highlight a common issue many jurisdictions are facing as their data protection laws come into effect and as they begin enforcement.

On one hand, the new regulations highlight key concepts regulators seek to better protect and implement more requirements: biometric identifiers and information about minors. On the other hand, the new regulations look to avoid penalizing businesses that are taking good faith efforts to comply with new laws via the opinion letter request process.

Businesses should continue to monitor Colorado and other U.S. states with data protection laws in effect as regulators shape and mold the coming enforcement of these new laws.

As U.S. states continue implementing and tweaking the new slate of broad data protection laws, the Benesch Data Protection and Privacy team is committed to staying at the forefront

of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.