BCLP. Client Intelligent

Insights

COLORADO'S CHILDREN'S PRIVACY AMENDMENTS – A COMPLIANCE CHECK AT THE SIX-MONTH MARK

Apr 28, 2026

In May 2024, Colorado Governor Jared Polis signed into law Senate Bill 41, which amended the Colorado Privacy Act (CPA) to create new protections for personal information of minors. SB 41 also introduced biometric data requirements, which took effect in July 2025 and are addressed in our separate alert: 'Colorado's new requirements for biometric data: what businesses need to know'. Although the children's data amendments took effect on October 1, 2025, they have received limited attention from companies subject to the CPA or from Colorado regulators. These provisions should not be overlooked, however, as they add to a growing number of states turning their focus to minors' data — including data of minors under 18 rather than those under 13. As enforcement in this area inevitably picks up, organizations — including those not otherwise subject to the CPA — will need to review their practices with respect to minors' data and factor in Colorado's new requirements alongside those of other state laws.

EXPANDED SCOPE AND APPLICABILITY

The requirements added under SB 41 extend further than the scope of the broader CPA, which generally applies to organizations that have processed personal information of 100,000 Colorado residents in the previous year. By contrast, the children's data amendments apply to any company conducting business in Colorado or delivering commercial products or services intentionally targeted at Colorado residents, regardless of its physical presence in the state or the volume of children's data processed. And, unlike most other state privacy laws, the CPA as a whole applies to not-for-profit entities as well as to for-profit organizations, meaning a whole host of small organizations could be subject to these new children's data requirements.

The children's data provisions are enforced by the Colorado Attorney General and district attorneys under the existing enforcement framework of the CPA.

BROADER PROTECTIONS FOR MINORS

The amendments to the CPA pertaining to minors' data have significantly broadened the requirements for the collection and processing of this type of data. The CPA raises the age of

protection from 13 to 18. This definition brings personal information about teens—previously outside the scope of the federal Children's Online Privacy Protection Act (COPPA), the primary law governing children's data—under its regulatory umbrella if and to the extent an organization has actual knowledge or willfully disregards an individual's minor status. Factors that could demonstrate willful disregard include whether the organization has received credible information from a consumer or parent indicating the consumer is a minor, whether the service is directed to minors based on factors such as marketing practices or audience composition, and whether the controller categorizes a consumer as a minor for business or advertising purposes.

DUTY OF REASONABLE CARE

Under the amendments, companies must exercise reasonable care to avoid heightened risk of harm to minors arising from the design or operation of an online service, product, or feature. "Heightened risk of harm" encompasses reasonably foreseeable risks that could result in unfair or deceptive treatment of minors, financial, physical, or reputational injury, unauthorized disclosure of personal information due to a data breach, or intrusive or offensive invasions of privacy. This duty of care operates independently of the data protection assessment requirements discussed below to establish a baseline standard of conduct for all organizations processing minors' data.

CONSENT REQUIREMENTS AND PROCESSING RESTRICTIONS

The amendments also impose new consent requirements for certain collections and uses of minors' data. Informed, opt-in consent must be obtained before an organization can engage in the following activities to the extent it has (or should have) actual knowledge of the minor's age. For minors under the age of 13, consent must be obtained from a parent or guardian; minors between the ages of 13 and 17 may provide consent directly. Controllers may not process a minor's personal data for the following purposes absent such consent:

1. Processing personal information to use in targeted advertising;
2. Selling a minor's personal information;
3. Using personal information to profile a minor in order to make a decision that produces a legal effect;
4. Using personal information for purposes incompatible with those described at the time of collection;
5. Using personal information for longer than is reasonably necessary to provide the online service, product, or feature; and
6. Collecting precise geolocation data, which is treated as sensitive data in the minors' context, unless necessary to provide a specific service.

RESTRICTIONS ON HIGH-ENGAGEMENT DESIGN FEATURES

Absent consent, a controller may not use system design features intended to significantly increase, sustain, or extend a minor's use of an online service, product, or feature. Factors to consider when making this determination include whether the feature was intentionally designed to increase engagement, whether there is evidence of increased or addictive use, and the totality of the circumstances.

AGE GATING AND VERIFICATION

The law does not require controllers or processors to implement age verification or age-gating systems, nor does it mandate the collection of consumers' ages. However, businesses that choose to conduct commercially reasonable age estimation to identify minors are protected from liability for errors in age estimation, provided their efforts are in good faith and documented. Additionally, satisfying the verifiable parental consent requirements under COPPA is considered sufficient under this statute.

DATA PROTECTION ASSESSMENTS

Any company that offers online services, products, or features to consumers where they have actual knowledge, or willfully disregard, that such consumers are minors must conduct a data protection assessment if there is a heightened risk of harm to minors.

This assessment must specifically address the purpose of the service, the categories of minors' personal information processed, the reasons for processing such data, and any reasonably foreseeable heightened risks to minors. Companies are required to review and update these assessments whenever there is a material change in processing operations and must retain documentation for at least three years after processing ceases or until the service is no longer offered, whichever is longer. If an assessment identifies heightened risks to minors, the organization must implement a mitigation plan. These assessments are confidential and exempt from public disclosure under the Colorado Open Records Act, though they must be made available to the Colorado Attorney General upon request.

IMPLEMENTATION STRATEGY

As new requirements related to minors' data come into force, companies will need to rethink their current compliance efforts. Organizations subject to these amendments should consider the following steps:

- **Reassess Applicability.** The children's data amendments apply to any company conducting business in Colorado or targeting Colorado residents, regardless of the volume of data processed. Companies that previously fell outside the CPA's general 100,000-resident

threshold should evaluate whether they are now subject to these requirements. In addition, organizations that collect specific ages of users should consider whether they implement additional controls to prevent the collection of all minor data and/or whether a particular collection (e.g., birthday reward that includes year of birth) is actually necessary for a particular activity, unless they are prepared to meet these new requirements.

- **Expand Age Protections Beyond 13.** Companies that have built their compliance programs solely around COPPA's under-13 framework should extend consent mechanisms and data handling practices to cover minors aged 13 through 17.
- **Implement Tiered Consent Mechanisms.** Companies should design consent flows that distinguish between age brackets (under 13 and 13 to 17) and confirm that consent mechanisms do not undermine, impair, or manipulate user autonomy and decision-making.
- **Review Product Design for High-Engagement Features.** Organizations should evaluate whether any design features (e.g., autoplay, infinite scroll, push notifications, and reward loops) are intended to significantly increase, sustain, or extend a minor's use of a service.
- **Conduct and Document Data Protection Assessments**. Companies should build repeatable assessment frameworks, retain documentation for at least three years after processing ceases, and be prepared to produce assessments to the Colorado Attorney General upon request. This process should also include mitigation plans for activities identified as providing a heightened risk to minors.
- **Monitor Enforcement Developments.** Companies should stay current on enforcement actions and guidance that may further clarify compliance expectations and also work to develop a strategy that works across all state laws rather than addressing requirements on a piecemeal basis.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Partner; Chair – Global Data Privacy and Security Practice; and Global Practice Group Leader – Technology, Commercial & Data, Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Goli Mahdavi

Global AI Lead, San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448

Andrea Rastelli

Associate, Boulder

andrea.rastelli@bclplaw.com

+1 303 417 8564
