Colorado Unveils New Privacy Rules: What Businesses – Including Employers – Need to Know to Stay Compliant

Insights
12.12.24

The Colorado attorney general's office just adopted significant updates to the Colorado Privacy Act (CPA) rules, which will soon introduce new obligations related to biometric data, employee biometrics, children's privacy, and interpretive guidance. These changes announced on December 6 mark a notable shift in Colorado's privacy landscape, requiring businesses – including employers – to address the collection and use of employee biometric data under privacy law for the first time. The new rules also refine protections for children's data and outline how businesses can seek legal clarity through opinion letters and interpretive guidance. While the changes aren't groundbreaking, they introduce practical compliance challenges for businesses operating in Colorado beginning the middle of 2025. With implementation deadlines on the horizon, now is the time for your organization to prepare. What are the key changes you need to know about, and what steps should you take?

Quick Background

Before we dive into the changes you need to know, let's provide a quick lay of the land. State lawmakers amended the CPA earlier this year to introduce privacy requirements for biometric information and enhance protections for minors' data. The Department of Law then introduced proposed rules in September to create contours around these new obligations. The Department received public comments for several months before releasing modified final rules last week. You can read more detail about the process here.

Key Changes Ushered in By the CPA Rules

With the finalization of these rules, there are three key changes to Colorado's data privacy landscape that all businesses should note.

1. New Notice and Consent Obligations for Biometric Privacy

Effective July 1, 2025, entities collecting biometric data (fingerprints, voiceprints, retina or iris scans, facial mapping, facial geometry, facial templates, etc.) must meet stringent notice and consent requirements if they use or intend to use it for unique identification.

- **Biometric Identifier Notice**: Data Controllers (or as defined by the CPA, a person that, alone or jointly with others, determines the purposes for and means of processing personal data) must

provide notice to individuals before collecting biometric identifiers, detailing what data is collected, why it's needed, how long it will be retained, and whether it will be shared. This notice can either stand alone or be integrated into your broader privacy notices – but it must be clearly labeled and accessible. And it must be an affirmative, informed acceptance.

- **Employee Biometric Data**: For the first time, employers must obtain written or electronic consent from Colorado employees before collecting their biometric data. They must also secure fresh consent if the data will be used for a new purpose or involves additional types of biometric identifiers.

The law does not consider digital or physical photographs, or audio or voice recordings, to be considered biometric data – unless, of course, the biometric identifiers with them are used for identification purposes.

2. Children's Privacy Protections

Effective October 1, 2025, entities offering online services, products, or features to a consumer whom a Controller actually knows or willfully disregards is a minors must:

- Obtain parental or guardian consent before processing a minor's data.
- Conduct data protection assessments for any features designed to significantly increase minors' use of a product or service.
- Limit the duration of data retention and avoid using system design features to manipulate minors' engagement.

3. Opinion Letters and Interpretive Guidance

Businesses soon can request opinion letters and interpretive guidance from the Attorney General to clarify their CPA compliance obligations. These letters could be valuable tool for businesses and employers, as they could provide a "good faith reliance defense" – even for entities not directly involved in the request at the Attorney General's discretion. This marks a change in protocol as previously such letters were only valuable to those organizations that had requested them. Another bit of good news: requesting such a letter will not impact the confidentiality of submitted data protection assessments and will not waive any sort of legal privilege or work product protection.

What's Next?

While we expect these finalized rules to remain largely intact, the Department of Law still needs the Colorado Attorney General to sign off on the final rules. Once that happens, the rules officially will be adopted and take effect 30 days after the Secretary of State publishes them. We'll monitor the situation and provide updates as warranted.

5 Pieces of Practical Guidance for Colorado Businesses

Like under the original CPA, any violations of the updated rules may be enforced by the Colorado Attorney General and district attorneys. For this reason, you should make sure to take these changes seriously. In the wake of these new challenges and opportunities, consider the following five steps to help you navigate Colorado's new data privacy frontier.

1. Audit Your Data Collection and Use Practices

- Identify any biometric data collection processes and assess whether your systems comply with the new notice and consent rules.
- Review how you collect, store, and use both biometric and minors' data, and ensure you can demonstrate compliance with heightened protections. Keep in mind dissemination to third parties and ensure your consent and policies cover those uses.

2. Update Privacy Notices and Policies

- Ensure your privacy notice includes a clear, broad, accessible section addressing biometric identifiers, or draft a standalone biometrics policy.
- Review your technology use and ensure all biometric technology are covered by your privacy notice.
- For businesses interacting with minors, update policies to reflect data retention limits, parental consent mechanisms, and new data protection assessment requirements.

3. Train Employees and Review Internal Processes

- Educate your team about the new requirements, especially HR staff who handle employee biometric data.
- Establish procedures to refresh employee consents and address the use of biometric identifiers for new purposes.

4. Leverage Opinion Letters for Clarity

- Consider seeking an opinion letter from the Attorney General's office if you face uncertainty about compliance. These can provide valuable legal protection and guidance.
- Coordinate with your FP counsel to determine whether and how to request such a letter.
- Monitor the upcoming opinion letter landscape for compliance guidance leading up to the CPA amendment effective date.

5. Start Preparing Now

- With the new rules taking effect as early as July 2025, early preparation steps will ensure smooth compliance – and reduce the risk of penalties or legal disputes.

- Contact your FP counsel today to start the ball rolling.

Conclusion

We will closely monitor these new rules and provide updates as warranted, so make sure you are signed up to receive Fisher Phillips Insights to receive the latest news direct to your inbox. If you have any questions regarding how data privacy laws can impact your business and steps for compliance, please reach out to your FP attorney, the authors of this Insight, or any member of Fisher Phillips' Privacy and Cyber Practice Group.

Related People

Danielle Kays
Partner
312.260.4751
Email

Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Associate
858.964.1582
Email

Danielle S. Urban, CIPP/E
Partner
303.218.3650
Email

Service Focus

Privacy and Cyber

Related Offices

Denver