Landmark Privacy Regulations Could Soon Require Colorado Employers to Comply With Biometric Info Law: 3 Tips to Stay Protected

Insights
10.03.24

Colorado employers could soon need to comply with the disclosure and consent requirements of the state's privacy act when they collect biometric identifiers from employees or applicants – which would make Colorado the first state outside of California to impose such obligations on employers. The state Attorney General's proposed regulations for the Colorado Privacy Act (CPA), released on September 13, would mark a huge change in the CPA, which currently does not apply to employers or employees. This Insight will give you all you need to know and provide you with three tips you can use to prepare.

History of Regulations and Amendments

Since Governor Polis signed the CPA in 2021, three actions have amended or added to the Act:

- The AG's 2023 Regulations, effective July 1, 2023, introduced rules on profiling (i.e., automated processing of personal data that predicts or analyzes a person's behavior or personal characteristics), data protection assessments, a universal opt-out mechanism for Colorado residents, and transparency in privacy notices. Like the Act, these regulations only apply to businesses that either control or process the personal data of 100,000 Colorado residents per year or receive a revenue or discount from the sale of and processing or controlling of the personal data of 25,000 Colorado residents.
- House Bill 24-1130 (HB 1130), passed on May 31, 2024, and effective on July 1, 2025, expanded the Act by imposing privacy requirements for the collection of any biometric information or identifiers for *any* entity, including employers, that collects or controls the biometric identifiers of any Colorado resident. Most notably, it requires controllers to pay the consumer before selling that consumer's biometric data in addition to complying with additional notification requirements.
- Senate Bill 24-041 (SB 041), passed on May 14, 2024, and effective on October 1, 2025, enhanced protections for minors' data, by prohibiting the processing for targeted advertising, an undisclosed purpose, or a time period longer than necessary without parental or guardian consent. It also added requirements for what constitutes parental or guardian consent for the minor or child and requires businesses to use reasonable care when offering online services or products to a minor and conduct a data protection assessment for the offered service or product.

What Are The Proposed Obligations Employers Should Track?

Under the proposed regulations, employers would only be able to require the collection of an employee's or applicant's biometric identifiers for the following purposes:

1. Access to secure physical locations and electronic systems;
2. Timekeeping; or
3. Improving or monitoring workplace safety generally or the public's safety in an emergency.

What are Biometric Identifiers?

Biometric identifiers are data from an individual's biological, physical, or behavioral traits used for identification. These include fingerprints, voiceprints, retina or iris scans, facial mapping, facial geometry, facial template, or other unique biological, physical, or behavioral characteristic or pattern.

Notice and Consent Requirements for Biometric Identifiers

The proposed regulations also incorporate the 2023 Regulations from the AG. That means, if finalized, a biometric data policy must be written to include a retention schedule, protocol when responding to a data security breach incident, and guidelines for deletion.

When a consumer – which soon include employees and applicants – exercises their right to access the collected biometric identifier(s), you would have to provide the following:

- Source from which the controller collected the biometric data;
- Purpose for which the controller collected or processed the biometric data and any associated personal data;
- Identity of any third party with which the controller disclosed or discloses the biometric data and the purposes for disclosing; and
- The category or category or description of the specific biometric data that the controller discloses to third parties.

Consent would need to meet the notice and consent requirements of the 2023 Regulations. This means the consumer's consent must be clear, affirmative, freely given, specific, and informed. Also, the notice must be reasonably accessible, meaning it must either be made available prior to collection or processing or linked from your homepage or a mobile app's store page/download page.

Regulations Specific to Children/Minors

The proposed regulations also incorporate SB 041's protections for minors' data, specifically

imposing consent requirements and data protection assessments for them.

For **consent**, controllers would be required to gain parental or guardian consent prior to:

- Processing a minor's personal data;
- Using any system design feature to significantly increase a minor's use of an online service or product; and
- Selling or disclosing biometric information (subject to HB 1130 exceptions).

Data protection assessments would need to consider minors and include the category of a minor's or child's personal data collected, the source, and any foreseeable risks of harm. These assessments would be required for activities starting after October 1, 2025.

When Will The New Regulations Take Effect?

These regulations are scheduled to take effect on July 1, 2025, after public comment period and hearing on the proposed regulations. The comment period will run from September 25 to November 7. Depending on the public comments, the Colorado AG's office may amend these proposed rules, so we'll track the status and provide an update when finalized.

3 Tips for Employers

While these new regulations are not yet finalized, and others take effect next year, preparing for these changes will take time and coordination. Here are three tips to start early and stay protected:

1. **Review and Evaluate Your Biometric Identifiers Consent Procedures**. Considering that biometric identifiers for employees and job applicants and the data from children and minors are receiving new focus from the AG, it is crucial for you to know the biometric identifiers you collect of employees or applicants. You'll also need to know whether that collection falls into one of the three allowed purposes of collection when evaluating your compliance and consent procedures.
2. **Update Privacy Policies**. Review your privacy policies to ensure that they comply with these new privacy laws including the requirements for accessibility and clear, understandable language. Coordinate with your FP Privacy counsel to ensure your policies are compliant with the new regulations before they take effect.
3. **Evaluate Your Audience's Age Range.** The regulations will impose heightened requirements for children's or minor's personal data and biometric identifiers that your business knows (or disregards) belongs to a minor. If you received information indicating the data you are processing belongs to a minor, this could mean you have knowledge – and will be required to comply under these requirements.

Conclusion

We will closely monitor this legislation 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

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

Kate Dedenbach, CIPP/US
Of Counsel
248.901.0301
Email

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

Rachel Song
Associate
415.926.7651
Email

Service Focus

Privacy and Cyber

Related Offices

Denver