CLIENT ALERTS & INSIGHTS

Colorado Amends Privacy Act to Include Enhanced Biometric Data Requirements

JUNE 11, 2024

The Colorado Privacy Act already required prior consent for sensitive personal data, with the amendment now setting forth requirements for purchasing and retaining biometric data.

The Colorado state legislature recently passed an amendment to the Colorado Privacy Act. The Colorado Privacy Act previously established the third broad data protection law in the U.S., after California and Virginia.

The Colorado Privacy Act came into effect July 1, 2023, and with it, requirements that in-scope businesses have fulsome and transparent privacy notices, obtain prior consent for processing of sensitive personal data, and implement broad data security requirements-including data protection impact assessment.

Colorado now also joins California-at least with respect to biometric data-as the only U.S. state data protection laws that impose at least some requirements on employee personal information. With the new slate of biometric data amendments, the Colorado Privacy Act now applies to an employer's use of employee and independent contractor biometric data.

Like the landmark Illinois Biometric Information Privacy Act, the biometric data amendments to the Colorado Privacy Act require a business to transparently disclose to consumers how biometric data is collected, used and shared by the applicable business. Unlike the Illinois Biometric Information Privacy Act, there is no private right of action allowing consumers to sue businesses for violations of the Colorado law.

The new biometric data requirements will apply to any business operating in Colorado and collecting ***any*** biometric data about Colorado consumers. The traditional Colorado law applicability thresholds do not apply.

Below, we dive into the applicable definitions and an overview of the new requirements set forth under the Colorado Privacy Act with respect to biometric information. For more information on the growing number of U.S. states with broad data protection laws in place, see the "U.S. State Privacy Laws" landing page.

Applicable Definitions

"Biometric data" means one or more biometric identifiers used or intended to be used for the purpose of identifying an individual.

"Biometric identifier" is then subsequently defined as any 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).

Importantly, biometric data does **not** include digital or physical photographs, audio or voice records, or data generated from such photographs or recordings. The definitions are critical in understanding how the new biometric requirements may apply to your business.

New Requirements

1. Privacy Policies and Notices

Privacy notices have become ubiquitous and are often the first step businesses take to comply with the growing number of U.S. state data protection laws.

The biometric data amendments, however, add a spin on the traditional public-facing privacy notice requirement by building in a new biometric-specific element.

First, the biometric data amendments require in-scope businesses to implement an internal, written policy that includes:

- An established retention schedule for how long the business retains biometric identifiers and biometric data;
- Procedures and protocols for responding to data security incidents and breaches affecting biometric identifiers or biometric data (including notifications to affected individuals);
- Guidelines for deleting biometric identifiers and biometric data upon the earlier of (1) the date when the initial purpose for processing the biometric identifier has been satisfied; (2) 24 months after the consumer last interacted with the business; or (3) the earliest reasonably feasible date-which shall be no more than 45 days after a business determines that storage is no longer necessary.

Businesses must review their retention of biometric data annually, which then increases the chances a business will need to delete biometric data earlier than the 24 month maximum retention period.

Second, the policy must then be incorporated into the business's public-facing privacy notice, provided that the business does not need to be as detailed as the internal policy. For example, the actual security measures in place and technical safeguards in place to mitigate or respond to data breaches do not need to be made public.

1. Prohibitions and Data Subject Rights

Businesses subject to the new biometric data amendments are prohibited from collecting and processing biometric identifiers unless the business has informed the consumer-clearly and conspicuously:

- That biometric identifiers will be collected;

- The specific purposes for which biometric identifiers are collected;
- The period of time that biometric identifiers will be retained; and
- Who and for what reasons biometric identifiers are disclosed.

The above would-in theory-be captured in the public-facing privacy notice.

The new amendments also include strict prohibitions with respect to the processing of biometric identifiers and data. For example, businesses are strictly prohibited from selling biometric identifiers-whether or not a consumer's prior consent is obtained or whether or not opt-out options are provided.

When businesses meet certain thresholds, consumers also have the right (in addition to others set forth in the existing Colorado Privacy Act) to require the business disclose to them:

- The source from which the biometric data was collected;
- The purpose for which the biometric data was collected and subsequently processed (and any related personal data);
- The actual identities of third parties whom the biometric data was shared with, as well as the purpose for which the data was shared; and
- The specific biometric data disclosed to third parties.

Employee Biometric Data

As discussed above, Colorado now joins California in requiring-at least in some respects-employers to meet certain privacy and security requirements with respect to handling employee and independent contractor personal data. In this case, the Colorado Privacy Act will only apply to employers' collection and use of biometric data; not personal data more broadly.

Under the amended Colorado Privacy Act, employers are **prohibited** from requiring consent to collect biometric data from employees and independent contractors, except where the biometric data is processed for the following purposes:

- Access control and security of facilities, hardware or software applications;
- Keeping time (punch clocks);
- Improving workplace safety and security; or
- Improving or monitoring the safety or security of public events.

Biometric data can be collected about employees or independent contractors for other purposes outside of those listed above, but that consent **cannot** be required as a condition for employment.

Importantly, employers are expressly **prohibited**

from using biometric data for the purpose of tracking a current employee's or independent contractor's location or how much time an employee or independent contractor spends on a piece of hardware or software.

Conclusion

All broad U.S. state data protection laws currently in effect or soon to be in effect include biometric data in their definitions of what is considered "sensitive". Additionally, many of those laws-including the Colorado Privacy Act-require a business to obtain a consumer's express, opt-in consent prior to collecting or processing sensitive personal data (subject to some exceptions). In this respect, the Colorado Privacy Act was already aligned to other state biometric -specific laws (such as the Illinois Biometric Information Privacy Act.

However, the biometric data amendment to the Colorado Privacy Act adds new, novel requirements that previous U.S. state data protection laws and biometric-specific laws have not previously directly addressed. Businesses that are collecting biometric data from consumers should take note and start to build out biometric data specific portions to their privacy notices.

Additionally, businesses who are not subject to the biometric data amendments to the Colorado Privacy Act should still take note and watch this space closely. Other states have been quick to take up and replicate new data protection requirements, so it would not be surprising to see more states follow in Colorado's footsteps.

As more states continue to implement their own variations of data protection laws and business' juggle the various requirements, 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.