



Privacy & Cybersecurity Update

June 2024

Colorado Adds Biometric Data Requirements to Privacy Law

On May 31, 2024, Colorado Governor Jared Polis signed into law [House Bill \(HB\) 1130](#), which amends the Colorado Privacy Act to create new requirements specific to collecting and processing biometric data. Importantly, the law creates biometric processing frameworks applicable to consumers and in the employment context. Unlike other biometric privacy laws, HB 1130 has no private right of action. It enters into force on July 1, 2025.

Defining Biometric Data

HB 1130 defines “biometric data” in a manner that is similar to other data protection laws. Specifically, the term biometric data essentially means information or data generated by the technological processing, measurement, or analysis of a person’s biological, physical, or behavioral characteristics (e.g., fingerprint, voiceprint, retina scans) used or intended for identification purposes. The term does not include digital or physical photographs, audio or voice recordings, or data generated therefrom.

Written Policies

HB 1130 mandates that a covered entity that processes biometric identifiers must adopt a written policy which establishes a retention schedule for the data and includes a protocol for responding to a data breach impacting biometric identifiers, including a consumer breach notification framework. A written policy must also comply with guidelines requiring the permanent destruction of biometric identifiers by the following timeframes: the earlier of (i) when the initial purpose of the collection has been satisfied, (ii) twenty-four months after the applicable

consumer interacted with the entity, or (iii) the earliest reasonably feasible date, which must be no more than 45 days after a covered entity determines that storing the biometric identifier is no longer necessary or relevant to the express processing purpose, as identified by an annual review. However, it may extend the 45-day period by up to 45 additional days, if necessary, given the complexity and number of biometric identifiers requiring deletion.

A covered entity must make its policy “available to the public,” which mirrors requirements found in other biometric privacy laws, provided HB 1130 does not require this public notice concerning biometric data processing that applies only to its current employees and is used solely for the entity’s operation. It is also not required to disclose its incident response plan publicly.

A covered entity does not have to adhere to its written policy when otherwise seeking to comply with certain types of warrants or compulsory requests or demands issued by certain government agencies.

Notice, Compliance, and Consent

Like other biometric data privacy laws, HB 1130 includes notice and consent requirements. Specifically, under the law, a covered entity is prohibited from collecting or processing biometric identifiers unless it first satisfies all the requirements under section 6-1-1308 of the Colorado Privacy Act, which are (at least in some instances) redundant to the requirements set forth elsewhere in HB 1130. For instance, section 6-1-1308 requires covered entities to comply with the following:

- **Duty of transparency.** A covered entity must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that describes its data processing activities.
- **Duty of purpose specification.** A covered entity must specify the express purposes for collecting and processing personal data.
- **Duty of data minimization.** A covered entity's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary for the specified purposes of processing the data.
- **Duty to avoid secondary use.** A covered entity must not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed unless the covered entity first obtains the consumer's consent.
- **Duty of care.** A covered entity must take reasonable measures to secure personal data during both storage and use from unauthorized acquisition. The data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business.
- **Duty to avoid unlawful discrimination.** A covered entity must not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.
- **Duty regarding sensitive data.** A covered entity must not process a consumer's sensitive data without first obtaining the consumer's consent or, in the case of the processing of personal data concerning a known child, without first obtaining consent from the child's parent or lawful guardian.

Prior to collecting or processing biometric identifiers, a covered entity must also clearly inform the consumer of the following: (i) that a biometric identifier is being collected, (ii) the purpose of the collection, (iii) the retention timeframe for such data by the covered entities, (iv) the business name of any processor to which the data will be disclosed, redisclosed, or otherwise disseminated, and (v) the specific purpose for which the biometric identifiers are being shared with a processor.

Lastly, when collecting or processing biometric identifiers, a covered entity must obtain the applicable person's consent, or when dealing with a known child, consent from the child's parent or legal guardian.

Other Prohibited Activities

HB 1130 prohibits both covered entities and the recipients of such biometric identifiers, from selling, leasing, or trading biometric identifiers, disclosing, or otherwise disseminating biometric identifiers unless the consumer (or their legal representative) consents to the activity, or they request the same to complete a financial transaction, or the disclosure, redisclosure, or dissemination to a processor and if necessary for the purpose for which the biometric identifier was collected or to which consent was given. Such activity is also permitted when the covered entity or receipt complies with state or federal law.

Like the Colorado Privacy Act, a covered entity is prohibited from discriminating against a person (e.g., refusing to provide goods or services, charging different prices) based on their refusal to furnish their biometric data for collection, subject to certain exceptions.

Purchasing Biometric Data

HB 1130 prohibits a covered entity from purchasing a biometric identifier, unless (i) the covered entity pays the consumer for the data, (ii) the purchase is unrelated to a product or service provision to the consumer, (iii) and the covered entity has obtained lawful consent.

Privacy Rights and (More) Notice Requirements

HB 1130 provides additional requirements for organizations that process and sell a large volume of biometric data. Specifically, it provides that a covered entity must "update the biometric identifier" within its custody or control, as requested by the consumer. It provides that the covered entity must "complete the update and delete any replaced data within sixty days after receiving the request" from the consumer. Further, subject to certain exceptions, a covered entity that collects a consumer's biometric identifiers must disclose to them, free of charge, the following:

- The category or description of the consumer's biometric identifier.
- The source from where the biometric data was collected.

- The purpose for which the covered entity used the identifier “and any associated personal data.”
- The identity of any third party with which the covered entity shares or has shared biometric data and the purpose for the sharing.
- The category or a description of the specific biometric identifiers that the covered entity discloses to third parties.

These update, deletion, and notice requirements, however, only apply to certain legal entities that (i) conduct business in, or produce or deliver commercial products or services that are marketed to residents of, Colorado, (ii) collect biometric identifiers or have biometric identifiers collected on its behalf, and (iii) either collects or processes the personal data of 100,000 individuals or more during a calendar year, *and* processes the personal data of 25,000 individuals or more and derives revenue from, or receives a discount on the price of goods or services from, the sale of personal data.

Processor Obligations

Importantly, HB 1130 requires a data processor to “satisfy” all the notice, compliance, and consent requirements listed above, provided that such a processor is **not** legally required to obtain consent directly from consumers (or their legal representatives) if the covered entity has obtained such consent and has otherwise complied with certain notice requirements in the law. Accordingly, it will be important for data processors to contractually require their customers (i.e., the covered entity) to make representations and warranties regarding the data they are processing and agree to remedies for breaches of the same.

Employees and Biometric Data

The new Colorado law introduces specific rules concerning the collection and processing of biometric data within employment settings. Specifically, an employer may require, as a condition of employment, that a current or prospective employee consent to allowing the employers to collect and process their biometric data only to:

- Permit access to secure physical locations, electronic hardware and software, provided it is not used for usage tracking purposes.
- Record the commencement and conclusion of the employee’s full workday, including meal and rest breaks over thirty minutes.
- Improve or monitor workplace safety or security to ensure the safety and security of employees.
- Improve or monitor the safety or security of the public in the event of an emergency or crisis situation.

An employer may collect and process biometric data for other purposes if (and only if) the employer obtains advance consent from the current or prospective employee. The law is clear that an employer may **not** require a current or prospective employee to consent to other such biometric data collection “as a condition of employment” or “retaliate” against a current or prospective employee who does not consent to such collection and processing.

HB 1130 incorporates the definition of “consent” from the Colorado Privacy Act. There, the term “consent” means “a clear, affirmative act signifying a consumer’s freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data.” The following does not constitute consent:

- Acceptance of a general or broad terms of use or similar documents that contain descriptions of personal data processing along with other unrelated information,
- Hovering over, muting, pausing, or closing a given piece of content, and
- Agreement is obtained through dark patterns.

Importantly, HB 1130 provides that its requirements cannot be interpreted to “restrict” an employer’s ability, or the ability of its processors, to collect and process biometric identifiers concerning a current or prospective employee if such an activity aligns with the reasonable expectation of an employee based on the employee’s job description or a prospective employee for purposes of obtaining a reasonable background check, application, or identification requirements.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky

216.566.5646

202.263.4126

Steve.Stransky@ThompsonHine.com

Certified Information Privacy Professional/Government (CIPP/G)

Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych

216.566.5605

Tom.Zych@ThompsonHine.com

Thora Knight, Ph.D.

212.908.3971

Thora.Knight@ThompsonHine.com

Marla M. Izbicky

312.998.4253

Marla.Izbicky@ThompsonHine.com

Certified Information Privacy Professional/United States (CIPP/US)

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2024 THOMPSON HINE LLP. ALL RIGHTS RESERVED.