CERIDIAN'S BIOMETRIC STATEMENT

This Statement was last updated on March 25, 2021

Scope

This statement applies to the processing of time and attendance-related information collected by timekeeping devices using finger scan, vein scan, and facial recognition technology ("biometric timekeeping devices"), Dayforce Touch, TUFF and Maximus, and shared with Ceridian by its customers, that may be considered biometric data or biometric data pursuant to certain states' laws. For more information on Ceridian's privacy practices please review our Global Privacy Statement.

California Residents: Ceridian processes your information as a service provider on behalf of Ceridian customers (your employer). You may have rights regarding your information under California law. For more information on your rights please contact your employer.

Definitions

Ceridian's use of the term "**biometric data"** within this statement does not reference any particular legal definition of that term. Instead, Ceridian's use of the term biometric data refers to the data collected by Ceridian's biometric timekeeping devices. It is the responsibility of Ceridian's customers to determine if applicable data protection and biometric privacy laws apply to the customer's use of Ceridian's biometric timekeeping devices.

How We Process Biometric Data

Ceridian processes the biometric data of its customers' employees at the direction of its customers through the use of a clock as part of a timekeeping system. The method by which Ceridian processes biometric data depends on the type of clock a customer is using:

> **Finger Scan Clocks** use multiple wavelengths of light to identify certain unique points on a user's finger. The clock then creates a code based on these unique data points associated with the user.
>
> **Vein Scan Clocks** use multiple wavelengths of light to identify certain unique patterns in the users' finger vein system. The clock then creates a unique code based on the unique vein patterns on each finger.
>
> **Face Verification Clocks** take a photograph of the user's face, for purposes of visual verification of identity, the device then plots key aspects of the face using the photograph to generate a unique code associated with the user.

For each type of clock, the data collected is converted into an alpha-numeric "Template Value" using a proprietary algorithm. Each time an individual uses the clock, it creates a temporary Template Value which is compared to the user's original Template Value. The original Template Value is stored on the clock and it is also sent to Ceridian and stored in the application database. Customer's may also choose to send photographs to Ceridian through Face Verification Clocks. Each temporary Template Value is stored only momentarily on the clock.

Consent

If consent is required to collect, store and or use the data processed by Ceridian biometric timekeeping devices under any applicable laws, Ceridian relies on its customers to obtain such consent or determine

another lawful basis for processing biometric data. Ceridian may also obtain separate written consent for the collection, storage and/or use of this information.

How We Use Biometric Data

Ceridian processes biometric data only on behalf of and at the direction of its customers. Ceridian's customers may choose to use clocks to track time and attendance of their employees.

Retention and Disposal

Biometric data is securely stored on the clock and in the Ceridian application database. A user's biometric data is deleted from the clock when the user's status is changed to terminated or when a badge is no longer valid. A user's biometric data is retained in the application database until 90 days after the customer changes the user's status to terminated or a badge is no longer valid. Biometric data may also be stored in archives. Archived biometric data will be stored by Ceridian no longer than 3 years after the date the biometric data is deleted from the application database.

How We Share Biometric Data

Ceridian does not sell, lease, trade or otherwise profit from biometric data. Ceridian does not authorize its vendors or customers to: use biometric data in a manner inconsistent with this Statement or Ceridian's Global Privacy Statement; or sell, disclose, lease, trade or otherwise profit from biometric data.

Biometric data may be accessed by Ceridian, its subsidiaries and third-party consultants to implement and manage the services of its customers. Ceridian affiliates and contractors, including ArcX, may have access to biometric data to perform maintenance on the biometric clocks. Some parties with which Ceridian shares biometric data may be outside of the jurisdiction in which the biometric data is collected. Where necessary, Ceridian enters into appropriate lawful data transfer agreements to process biometric data outside of the jurisdiction in which it was collected.

Ceridian will not share biometric data with any other third party unless:

- The customer's employee or the employee's authorized representative provides written consent to share;
- Disclosure is permitted or required by applicable law or is in response to subpoenas, court orders, or other legal processes.