Biometric Data Privacy Policy

TimeTrak Privacy Policy for the Processing of Biometric Data

TimeTrak Systems, Inc. ("TimeTrak") has instituted the following policy related to any U.S. resident biometric data that is collected, processed and/or stored by TimeTrak or is subject to the requirements of any law expressly governing the collection, storage, use and/or disclosure of biometric data.

Not all TimeTrak products and services utilize biometric technologies, and not all TimeTrak's biometric technology products and services involve TimeTrak in the collection, storage or use of biometric data. In some cases, TimeTrak may provide hosting services for certain biometric data collected by a customer of TimeTrak ("Customer") on such Customer's behalf. In other cases, TimeTrak products are installed on the Customer's computers and servers where TimeTrak is not involved in the participation of the collection, storage or use of biometric data. The Customer decides if it purchases a product that utilizes biometric data, and whether such data is collected, stored or utilized by Customer or TimeTrak.

Biometric Information

The biometric data covered by this policy includes "Biometric Identifiers" as defined by BIPA (including, a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) and "Biometric Information" as defined by BIPA (i.e., any information, regardless of how it is captured, converted, stored, or shared, based on an individual's Biometric Identifier used to identify an individual).

At the direction and on behalf of its Customers, TimeTrak may collect, store and/or use biometric data. Customers may utilize TimeTrak's products and services to collect, store and/or use biometric data for employment-related purposes, including but not limited to verifying and identifying employees for purposes of tracking of time and attendance, in accordance with this policy and applicable law.

Biometric Devices (a "Device") purchased by a Customer for time tracking or other intended purposes, use biometric technology to recognize and record Biometric Identifiers from individuals who interact with the Device.

When an individual enrolls with, or authenticates themselves to, the Device, the Device temporarily captures and stores an image of that individual's biometric identifier, either the individual's face or fingerprint, (the "Identifier") but only for the time needed to create the individual's biometric template (the "Template") used for subsequently recognizing that same individual.

Thereafter, only the Template, which is a binary computer file (not an image file) representing a tiny subset of the individual's Identifier, is stored.

After an individual's Template is generated, the individual's Identifier (the image of the employee's face or fingerprint) is used to create a low-resolution (the "thumbnail") that is used to ensure proper alignment, framing, lighting, and exposure of the identifier. The original high resolution identifier image is immediately and permanently deleted from the Device.

The individual's Identifier is temporarily stored during the process of generating the Template and the Device does not permanently store an any Identifier.

All Templates stored in the Device's operating software are stored using encryption algorithms and are stored in the encrypted state. All Templates stored within the TimeTrak software, either cloud hosted or installed on-premises at the Customer, are stored in the encrypted state in transit and at rest.

Customer's Responsibilities

It is the sole responsibility of the Customer that collects, captures, stores, or otherwise uses Biometric Data relating to an individual, whether using TimeTrak's cloud hosted products and services or using TimeTrak's products installed locally on the customers' computers and servers, to do each of the following:

1. Inform the individual (i.e. employee, supervisor, end-user) from whom Biometric Data will be collected, in writing and prior to collecting the individual's Biometric Data, that Biometric Data is being collected, stored, and/or used.
2. Indicate, in writing, the specific purpose(s) and length of time for which Biometric Data is being collected, stored, and/or used.
3. Receive a written consent and release from the individual (or a legally authorized representative) authorizing the Customer and TimeTrak to collect, store, and/or use the Biometric Data and authorizing the Customer to disclose such Biometric Data to TimeTrak and any Customer third-party service providers for use and storage pursuant to this Policy.
4. Delete Biometric Data from TimeTrak products, using tools provided by TimeTrak, on termination of employment consistent with the Customer's Biometric Data Privacy Policy and all application laws.
5. Develop, maintain, and inform all individuals about any Customer policies for Biometric Data collection. The Customer must maintain its own data collection, disclosure, retention, and storage policies in compliance with all applicable laws. Where required by law, Customer agrees to adopt a privacy policy in alignment with all applicable laws governing the collection, use, transfer and retention of Personal Data.
6. Ensure that TimeTrak is immediately notified of use of, or discontinuation of use of, TimeTrak's products or services involved in the collection, storage or use of biometric data.

Disclosure and Sharing of Biometric Information

TimeTrak will not sell, lease, trade or otherwise profit from any biometric data that it receives from Customer's employees. Biometric data will not be used for any purpose other than as described herein.

TimeTrak will not disclose, redisclose or otherwise disseminate any biometric data received from Customers to any person or entity other than TimeTrak and TimeTrak System's third party service providers except for if disclosure or redisclosure is required by state or federal law or municipal ordinance or disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Regarding Illinois Biometric Information Privacy Act

In accordance with the Illinois Biometric Information Privacy Act (740 Ill. Comp. Stat. Ann. 14/1 et seq.) (the "Illinois BIPA"), TimeTrak maintains comprehensive policies and procedures to ensure the proper collection, use, safeguarding, storage, retention, and destruction of Biometric Data by TimeTrak. As required by the Illinois BIPA, TimeTrak makes available its Retention of Biometric Data Retention and Storage of Biometric Information as set forth below. These policies apply to all Customer Personal Data, not just Customer Personal Data collected in Illinois, and only apply to TimeTrak Cloud Hosted products and services. These policies do not apply to TimeTrak products installed on the customers' computers and servers not controlled by TimeTrak and the Customer is responsible for all Biometric Information and Retention and Storage.

Retention of Biometric Information

TimeTrak may retain biometric data for up to ninety-three (93) days after receiving notice from customers on the discontinuation of use of TimeTrak products and services. TimeTrak shall permanently destroy all copies of the employee's Biometric Data in its possession after the time period has elapsed, unless TimeTrak is required to hold Customer Personal Data pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Storage of Biometric Information

TimeTrak will use a reasonable standard of care, consistent with the industry in which TimeTrak operates, to store, transmit and protect from disclosure all biometric data, and shall store, transmit, and protect from disclosure all biometric data in a manner that is the same as or more protective than the manner in which TimeTrak stores, transmits, and protects other confidential or sensitive data that can be used to uniquely identify an individual or an individual's account.