Biometric Data Policy

Last revised and effective as of August 2nd, 2023

Introduction

At MPAY, Inc., doing business as Payentry ("MPAY/Payentry, "we" or "us" or "our"), we are committed to protecting the Biometric Data (as defined below) that we collect, possess, store, and use (collectively, "process"). We process Biometric Data solely on behalf of and at the direction of our business clients that use our products and/or services (each, a "Client"). **Our Clients are responsible for developing and complying with their own biometric policies as may be required under applicable law.**

This Biometric Data Policy (this "Biometrics Policy") applies to (1) fingerprint and scan of hand or face geometry information ("biometric identifiers"); and (2) any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual, including a template value into which a biometric identifier is converted ("biometric information") (collectively, "Biometric Data") that we process in connection with providing our products and/or services to our Clients through our Client's Employee's use of our products and/or services. "Employee" as used in this Biometrics Policy means an employee, independent contractor, or other personnel of our Client.

For the avoidance of doubt, our Clients are responsible for providing notice to, and obtaining consent from, their Employees and for complying with applicable laws (including with respect to retention and destruction obligations) regarding the Biometric Data that they may collect or possess in connection with our products and/or services.

Purpose for Processing Biometric Data

Through the provision of our products and/or services to our Clients, we will process our Clients' Employees' Biometric Data. Specifically, we process Biometric Data for the purpose of fraud prevention to ensure the security and integrity of timekeeping services and associated mobile applications provided to our Clients. These timekeeping services and associated mobile applications utilize Biometric Data to authenticate the identity and record the activities of our Clients' Employees, such as when our Clients' Employees start or end a shift, or to handle time off requests. As part of authenticating the identities of our Clients' Employees, the biometric identifiers that we collect may be converted into template values. A template value is generated each time one of our Clients' Employees uses our timekeeping services and associated mobile application when biometric punch validation is enabled and is compared against the original template value generated when one of our Clients' Employees registers to first use our timekeeping services and associated mobile application.

Disclosure of Biometric Data

We do not sell, lease, trade, or otherwise profit from Biometric Data.

Other than to third-party service providers and to our Clients as described below, or as permitted by applicable law, we will only disclose, redisclose, or otherwise disseminate Biometric Data: (1) with a Client's Employee's consent; (2) where the disclosed Biometric Data completes a financial transaction requested or authorized by a Client's Employee; (3) as required by state or federal law or municipal ordinance; or (4) as required by a valid warrant or subpoena issued by a court of competent jurisdiction.

As part of providing our products and/or services to our Clients, we may disclose, redisclose, or otherwise disseminate Biometric Data to third-party service providers solely to provide our products and/or services. In particular, we may use Microsoft face recognition technology to process Biometric Data as a service provider.

In addition, we may disclose, redisclose, or otherwise disseminate an Employee's Biometric Data to the Client associated with that Employee.

Security

In processing Biometric Data, we use a reasonable standard of care to store, transmit, and protect from disclosure all Biometric Data, and shall store, transmit, and protect from disclosure Biometric Data in a manner that is the same as or more protective than the manner in which we store, transmit, and protect from disclosure other confidential and sensitive information.

Retention and Destruction

We will retain relevant Biometric Data only until the earlier of such time that our Client notifies us that (1) its Employee has been terminated; or (2) it has discontinued use of a product and/or service that utilizes Biometric Data. Upon receiving notice of either event, we will destroy the relevant Biometric Data within a reasonable period of time.

And upon receiving a written request from our Client to destroy Biometric Data, we will promptly comply with such a request regarding Biometric Data associated with that Client.

How to Contact Us

If you have any questions or comments about this Biometrics Policy, please contact us using any of the following:

Payentry or
MPAY, Inc.
Attn. Customer Care – Privacy Policy
19701 Bethel
Church Rd., Suite 103, Box 320
Cornelius, NC
28031
Phone: (888) 632-2940

To contact us via email, fill out the Contact form at the bottom of our website and we will get back to you.

Questions concerning a Client's privacy practices, including its use of Biometric Data, should be addressed to that Client.

For login assistance or technical support, please contact your employer or payroll administrator.