Biometric Information Privacy Act (BIPA)

Last Updated: September 20, 2022

Paylocity Corporation ("Paylocity", "our", "we" and "us")") has instituted the following policy related to any biometric data that we possess as a result of our operations or of our clients' and client employees' use of our products and services. Our clients are responsible for developing and complying with their own biometric data retention and destruction policies as may be required under applicable law.

Biometric Data Defined

As used in this policy, "biometric data" includes "biometric identifiers" and "biometric information" as defined in the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq. "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

"Biometric data" also includes any similar state or local law definitions related to any biological characteristics of a person, or information based upon such a characteristic, including but not limited to, "biometric identifier" as defined under Tex. Bus. & Com. Code §503.001, "biometric identifier" as used in Wash. Rev. Code Ann. §19.375.020, "biometric information" as used in the California Consumer Privacy Act, "biometric information" as used in the New York Stop Hacks and Improve Electronic Data Security Act, and "biometric data" as used in Arkansas Code §4-110-103.

Purpose for Collection of Biometric Data

Our clients are responsible for compliance with applicable law governing any collection, storage, use, and/or transmission of biometric data they conduct or facilitate. To the extent required by law, our clients will obtain written authorization from each employee for the benefit of the client, Paylocity and/or Paylocity's authorized licensors or vendors to collect, store, use, and/or transmit biometric data prior to the collection of such data.

Paylocity and/or its vendors also may collect, store, use and/or transmit biometric data during the course of conducting Paylocity's operations and of providing products or services to Paylocity's

clients and client employees. With respect to biometric data collected, stored, used and/or transmitted by Paylocity and/or its vendors, to the extent required by law, our clients will obtain written authorization from each employee for the benefit of Paylocity and/or Paylocity's authorized licensors or vendors to collect, store, use, and/or transmit biometric data prior to the collection of such data.

Paylocity and/or its vendors will collect, store, use and/or transmit any biometric data solely for identifying employees, recording time entries, identity verification, workplace security, and fraud prevention. Neither Paylocity nor its vendors will sell, lease or trade any biometric data that it receives from clients or client employees as a result of their use of Paylocity's services.

Authorization

To the extent that Paylocity, its vendors, and/or its clients collect, capture, or otherwise obtain biometric data relating to an employee, Paylocity's clients for the benefit of Paylocity must first:

- Inform the employee in writing that Paylocity, its vendors, and/or its clients are collecting, capturing, or otherwise obtaining the employee's biometric data, and that Paylocity may provide such biometric data to its vendors and its client;
- Inform the employee in writing of the specific purpose and length of time for which the employee's biometric data is being collected, stored, and used; and
- Receive a written release signed by the employee (or his or her legally authorized representative) authorizing Paylocity, its vendors, and/or its client to collect, store, and use the employee's biometric data for the specific purposes disclosed by Paylocity, and for Paylocity to provide such biometric data to its vendors and its client.

Paylocity, its vendors, and/or its clients will not sell, lease, trade, or otherwise profit from employees' biometric data; provided, however, that Paylocity may be paid for products or services used by Paylocity's vendors or clients that utilize such biometric data.

Disclosure

Paylocity will not disclose or disseminate any biometric data to anyone other than its authorized vendors and clients without/unless:

- the subject of the biometric data or the subject's legally authorized representative consents to the disclosure or dissemination;
- the disclosure or dissemination completes a financial transaction requested or authorized by the subject of the biometric data or the subject's legally authorized representative;
- the disclosure or dissemination is required by State or federal law or municipal ordinance; or
- the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

Paylocity shall retain any client's employee's biometric data in Paylocity's possession only until the first of the following occurs:

- Paylocity receives written notice from its client that the initial purpose for collecting or obtaining such biometric data has been satisfied, such as the termination of the employee's employment with Paylocity's client, the employee moves to a role within the client for which the biometric data is not used, or the client has discontinued using Paylocity's product or service for which the biometric data was used; or
- Within 3 years of Paylocity receiving written notice of the client's employee's last interaction with the client.

Data Storage

Paylocity and its vendors shall use a reasonable standard of care to store, transmit, and protect from disclosure any paper or electronic biometric data collected. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which Paylocity stores, transmits, and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as genetic markers, genetic testing information, account numbers, PINs, driver's license numbers and social security numbers.