Southshore
COMPANIES

Policy Information Security Policy/Employee Handbook, Section 5-23

DATE November 18, 2021

Part 4 Illinois Biometric Information Privacy Act ("BIPA") Policy

1. **Introduction**. Including, but not limited to; Southshore Enterprises, Inc., Southshore Distribution, LLC, United Container Co. (hereinafter referred to as "Southshore/United Container" or "Company" or "Employer") has instituted the following policy related to any biometric data that the Company processes during the ordinary course of business operations.

2. **Purpose**. To comply with the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq.

3. **Scope**. This Policy applies to all Company employees, temporary workers, and independent contractors. Additionally, this Policy applies to all persons who enter onto Company premises.

4. **Policy**

   4.1. 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.

      a. "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

      b. "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.

      c. "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.

4.2. Purpose for Collection of Biometric Data. The Company and/or its service providers (for example, its security camera provider, payroll provider, and/or temporary staffing agency) may collect, store, use and/or transmit biometric data during the ordinary course of Company business. With respect to biometric data collected, stored, used and/or transmitted by the Company, to the extent required by law, the Company will obtain written authorization from each employee for the benefit of the Company and/or the Company's authorized service providers to collect, store, use, and/or transmit biometric data prior to the collection of such data.

The Company and/or its service providers will collect, store, use and/or transmit any biometric data solely for identifying employees, identity verification, workplace security, and fraud prevention. Neither the Company nor its service providers will sell, lease or trade any biometric data that it receives from employees.

4.3. Retention Schedule. The Company shall retain any employee's biometric data in the Company's possession only until the first of the following occurs:

a. The Company determines that the initial purpose for collecting or obtaining such biometric data has been satisfied; or

b. Within 3 years of the Company's last interaction with an employee.

4.4. Data Storage. The Company 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 the Company 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.

5. Procedure

5.1. Authorization. To the extent that the Company and/or its service providers collect, capture, or otherwise obtain biometric data relating to an employee, the Company will first:

a. Inform the employee in writing that the Company and/or its service providers are collecting, capturing, or otherwise obtaining the employee's biometric data;

b. 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

c. Receive a written release signed by the employee (or his or her legally authorized representative) authorizing the Company and/or its service providers to collect, store, and use the employee's biometric data for the specific purposes disclosed by the Company, and for the Company to provide such biometric data to its service providers.

The Company and its service providers will not sell, lease, trade, or otherwise profit from employees' biometric data.

5.2. Disclosure. The Company will not disclose or disseminate any biometric data to anyone other than its authorized service providers without/unless:

a. the subject of the biometric data or the subject's legally authorized representative consents to the disclosure or dissemination;

b. 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;

c. the disclosure or dissemination is required by State or federal law or municipal ordinance; or

d. the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

6. Effective Date. This Policy is effective as of [DATE].

6.1. Revision History: [DATE]

Biometric Information Privacy Employee Consent Form

As a condition of employment, partnership, contract, or any relationship with Southshore Enterprises, Inc., Southshore Distribution, LLC, Red Marlin Logistics, LLC, and United Container Co., (hereinafter referred to as "Southshore/United Container" or "Company" or "Employer"), the person named below agrees to the following:

The person named below has been advised and understands that the Company and/or its service providers, collect, retain, and use biometric data for the purpose of identifying employees, identity verification, workplace security, and fraud prevention. Specifically, the Company has an internal CCTV system that may capture your face geometery that is provided and monitored by the Company's service providers. Moreover, the Company and its service providers collect, retain, and use biometric data for the purpose of recording time entries when utilizing the Company's biometric timeclocks or timeclock attachments. Biometric timeclocks are computer-based systems that scan an employee's finger for purposes of identification. The computer system extracts unique data points and creates a unique mathematical representation used to verify the employee's identity, for example, when the employee arrives at or departs from the workplace.

The Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), regulates the collection, storage, use, and retention of "biometric identifiers" and "biometric information." "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. "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.

The employee, independent contractor, or temporary worker understands that he or she is free to decline to provide biometric identifiers and biometric information to the Company, its service providers without any adverse employment action. The employee may revoke this consent at any time by notifying the Company in writing.

The undersigned employee acknowledges that he/she has received the attached *Illinois Biometric Information Privacy Act Policy*, and that he/she voluntarily consents to the Company's and/or its service providers' collection, storage, and use of biometric data, including to the extent that it utilizes the employee's biometric identifiers or biometric information as defined in BIPA, and voluntarily consents to the Company providing such biometric data to any service providers for the purpose of workplace security and the Company's time and attendance software.

_____

Employee/Individual Signature

_____

Printed Name

_____

Date