

Biometric Information Privacy Policy

Imperial Bag & Paper Co. LLC, dba Imperial Dade (the “Company”) maintains a time management system provided by Automatic Data Processing, Inc. (“ADP”), a third-party service provider that supports the time management system, to ensure all employee time is accurately captured.

The Company has established this biometric privacy policy to comply with the Illinois Biometric Information Privacy Act.

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.

Purpose for Collection of Biometric Data

The Company and/or ADP collects, stores, and uses employee biometric data for the purpose of administering the Company’s employee timekeeping system, including by verifying employee identity and ensuring that all hours worked are accurately recorded. These purposes shall include, but not be limited to, time management verification processes and related audits and investigations.

Disclosure and Authorization

To the extent that the Company and/or ADP collect, capture, or otherwise obtain biometric data relating to an employee, the Company must first:

- a. Inform the employee in writing that the Company and/or ADP are collecting, capturing, or otherwise obtaining the employee’s biometric data, and that the Company is providing such biometric data to ADP;

- 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 ADP 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 ADP.

The Company and/or ADP will not sell, lease, trade, or otherwise profit from employees' biometric data; provided, however, that ADP may be paid for products or services used by the Company that utilize such biometric data.

Disclosure

The Company will not disclose or disseminate any biometric data to anyone other than ADP without/unless:

- a. First obtaining written employee consent to such disclosure or dissemination;
- b. The disclosed data completes a financial transaction requested or authorized by the employee;
- c. Disclosure is required by state or federal law or municipal ordinance; or
- d. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

The Company shall retain employee biometric data only until, and shall request that ADP permanently destroy such data when, the first of the following occurs:

- The initial purpose for collecting or obtaining such biometric data has been satisfied, such as the termination of the employee's employment with the Company, or the employee moves to a role within the Company for which the biometric data is not used; or
- Within 3 years of the employee's last interaction with the Company.

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.