



Biometric Information Privacy Policy

Royal Die and Stamping, LLC (“the Company”) has instituted the following biometric information privacy policy:

A. 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 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.

B. Purpose for Collection of Biometric Data

The Company, directly or indirectly as a licensee/authorized user/purchaser of time and attendance software from third-party vendors (“its Vendors”) may collect, store, and use biometric data solely for employee identification, fraud prevention, and pre-employment hiring purposes.

C. Disclosure and Authorization

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

1. Inform the employee in writing that the Company and/or its Vendors are collecting, capturing, or otherwise obtaining data of employees, which constitute biometric data as defined under BIPA or other applicable law, and that the Company is providing such biometric data to its vendors from whom it licenses and/or acquires the use of time and attendance software;
2. Inform the employee in writing of the specific purpose and length of time for which the data, which may constitute biometric data as defined under BIPA or other applicable law, is being collected, stored, and used; and

3. Receive a written release signed by employees (or their respective legally authorized representatives) authorizing the Company and/or its Vendors 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 Vendors.

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

D. Disclosure

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

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

E. Retention Schedule

The Company shall retain employee biometric data only until, and shall request that its Vendors 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 three (3) years of the employee's last interaction with the Company.

F. 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 account numbers, PINs, driver's license numbers and social security numbers.

**RELEASE AUTHORIZING THE COLLECTION, STORAGE AND USE OF BIOMETRIC
DATA**

The employee named below (“Employee”) has been advised and understands that Royal Die & Stamping LLC (“the Company”) directly or indirectly as a licensee, authorized user, or purchaser, of time and attendance software from one or more third-party vendor (“its Vendors”), may collect, retain, and use biometric data, which may constitute biometric identifiers” and/or “biometric information” as those terms are defined in the Illinois Biometric Privacy Act, 740 ILS 14/1, *et seq.* (“BIPA”) or other applicable law.

The biometric data collected, retained and/or used by the Company and/or its Vendors is for the purpose of identifying employees and 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 (“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.

Employee understands that Employee is free to decline to provide biometric identifiers and biometric information to the Company and/or its Vendors without any adverse employment action. Employee may revoke this consent at any time by notifying the Company in writing.

Employee acknowledges that Employee has received the attached *Biometric Information Privacy Policy*, and that Employee voluntarily consents to the Company’s and/or its Vendors’ collection, storage, and use of biometric data through a biometric timeclock, including to the extent that it utilizes Employee’s biometric identifiers or biometric information as defined in BIPA, and voluntarily consents to such biometric data being transferred, exchanged or provided by and between Employee, Company and its Vendors.

Print Name: _____

Signature: _____

Date: _____