

BIOMETRIC INFORMATION NOTICE, CONSENT, AND RELEASE

(Mobile Timekeeping Application)

1. Purpose of This Agreement

This Biometric Information Notice, Consent, and Release (“Agreement”) explains how Soulé Software Corporation (“Company”) collects, uses, stores, and destroys biometric identifiers or biometric information, including a photographic biometric image captured through a mobile phone application, for purposes of timekeeping, payroll, jobsite access control, safety, and compliance.

By signing below, you acknowledge that you have read this Agreement, understand it, voluntarily consent to the collection and use of your biometric information as described, and waive and release any liability that may arise from the Company’s use of your biometric information for the purposes described.

2. Definition of Biometric Information

For purposes of this Agreement, “Biometric Information” includes, where permitted by law:

- A photograph or image of your face captured through a mobile application;
- Any facial geometry, facial mapping, or template derived from such image;
- Any data generated from the image that is used to uniquely identify you for timekeeping purposes.

Biometric Information does not include photographs used solely for identification badges or general security purposes unless converted into a biometric identifier.

3. Description of Technology

The Company uses a mobile phone application that may:

- Capture a photographic image of your face at the time you clock in and clock out;
- Analyze that image to verify your identity and prevent “buddy punching” or time fraud, and ensure that only authorized, safety-trained personnel are present on active job sites;
- Associate the biometric verification with your timekeeping and payroll records.

You acknowledge that the application may be provided by a third-party vendor acting as a service provider or processor on the Company’s behalf and that your Biometric Information may be processed and stored on secure cloud-based servers managed by such providers. No Biometric Information will be collected until after the execution of this Agreement.

4. Purpose and Legal Basis for Collection

Your Biometric Information is collected and used solely for the following legitimate business purposes:

- Accurate time tracking and payroll processing;

- Verification of employee or worker identity at job sites;
- Compliance with wage-and-hour, union, prevailing wage, and safety requirements;
- Protection of Company property and prevention of misuse of timekeeping systems.

The Company will not sell, lease, trade, or profit from your Biometric Information.

5. Storage, Safeguards, and Retention

The Company will:

- Store Biometric Information using reasonable administrative, physical, and technical safeguards consistent with industry standards;
- Limit access to Biometric Information to authorized personnel or vendors with a legitimate need;
- Retain Biometric Information only for as long as necessary to fulfill the purposes described above, or as required by law.

Unless a shorter period is required by applicable law (such as in Texas, where identifiers are destroyed within one year of the purpose being satisfied), Biometric Information will be permanently destroyed when the earliest of the following occurs:

- The initial purpose for collection has been satisfied; or
- Three (3) years after your last interaction with the Company via the application.

Notwithstanding the foregoing, the Company may retain Biometric Information for a longer period where retention is required to comply with a litigation hold, subpoena, court order, government investigation, audit, legal proceeding, or other legal-preservation obligation.

6. Disclosure to Third Parties

The Company may disclose Biometric Information only:

- To third-party application or payroll providers under written agreements requiring confidentiality, security, and compliance with applicable biometric laws;
- Where required by law, court order, or valid legal process;
- With your additional consent, if required by applicable law.

7. Voluntary Consent and Acknowledgment

By signing this Agreement, you:

- Voluntarily authorize and consent to the collection, capture, storage, use, and destruction of your Biometric Information as described;
- Acknowledge that you have been informed in writing of the purpose and length of time for which your Biometric Information will be collected, stored, and used;

- Understand that refusal to provide biometric consent may affect your ability to use this specific timekeeping method, and that alternative procedures may be available. If you decline to provide consent, you may request an alternative timekeeping method, which the Company will provide where required by law.

8. Waiver and Release

To the maximum extent permitted by applicable law, you hereby release and hold harmless the Company, its affiliates, officers, employees, agents, and vendors from any claims, damages, penalties, or causes of action arising out of the Company's good-faith collection and use of your Biometric Information in compliance with this Agreement and applicable law.

Nothing in this section is intended to waive any rights that cannot legally be waived under applicable federal, state, or local law.

9. Governing Law

This Agreement shall be governed by the laws of the state in which you primarily perform work for the Company, without regard to conflict-of-law principles, except where biometric statutes expressly mandate otherwise.

10. Acknowledgment and Signature

I acknowledge that I have read and understand this Biometric Information Notice, Consent, and Release and I agree to its terms, as well as any provisions in Addendum A which may apply to me. For purposes of this Agreement, the parties agree that electronic signatures and signatures delivered by facsimile shall have the same legal force and effect as manually executed original signatures.

Worker Name: _____

Signature: _____

Date: _____

Job Site / State(s) Worked In (if applicable): _____

ADDENDUM A

STATE-SPECIFIC BIOMETRIC INFORMATION NOTICE AND CONSENT

This Addendum supplements the Biometric Information Notice, Consent, and Release (“Agreement”) and applies only to employees or workers who reside in, work in, or whose biometric data is collected in the states identified below. In the event of a conflict, this Addendum controls.

1. Illinois – Biometric Information Privacy Act (BIPA)

This section applies to individuals covered by the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 et seq.

A. Written Notice

You are hereby notified that Soule Software Corp. collects, captures, stores, and uses biometric identifiers and/or biometric information, including a photographic biometric image and facial geometry, through a mobile application for timekeeping and related business purposes.

B. Purpose and Duration

Your Biometric Information is collected and used solely for:

- Employee or worker identity verification;
- Timekeeping and payroll administration;
- Jobsite compliance, fraud prevention, and safety.

Your Biometric Information will be retained only until the earliest of:

1. The initial purpose for collecting or obtaining such information has been satisfied; or
2. Three (3) years after your last interaction with the Company via the biometric timekeeping system.

C. No Sale or Disclosure for Profit

The Company will not sell, lease, trade, or otherwise profit from your Biometric Information.

D. Written Release

By signing this Agreement, you provide the written release required by BIPA, authorizing the Company to collect, store, use, and destroy your Biometric Information in accordance with the Agreement and this Addendum.

2. Texas – Capture or Use of Biometric Identifier Act (CUBI)

This section applies to individuals covered by Texas Bus. & Com. Code § 503.001.

The Company:

- Informs you that a biometric identifier (including facial geometry derived from a photographic image) is being captured;
- Uses the biometric identifier only for a commercial purpose reasonably related to employment;
- Will not sell or disclose the biometric identifier except as permitted by law;
- Will destroy the biometric identifier within a reasonable time, and no later than one (1) year after the purpose for collection has been satisfied, unless a shorter period is required by law.

By signing the Agreement, you consent to such collection and use.

3. Washington – Biometric Identifiers Law

This section applies to individuals covered by RCW 19.375.

The Company provides notice and obtains consent prior to enrolling your biometric identifier and:

- Uses the biometric identifier only for timekeeping, identity verification, and related operational purposes;
- Maintains reasonable care to protect biometric identifiers;
- Does not sell biometric identifiers or use them for purposes other than those disclosed.

4. California – CCPA / CPRA (Biometric Information as Sensitive Personal Information)

This section applies to individuals covered by the California Consumer Privacy Act, as amended by the California Privacy Rights Act.

A. Notice at Collection

Your Biometric Information constitutes Sensitive Personal Information under California law. The Company collects this information solely for employment-related purposes, including timekeeping, payroll, and fraud prevention.

B. Limited Use

The Company limits its use of Biometric Information to what is reasonably necessary and proportionate to achieve the disclosed purposes and does not use it for unrelated secondary purposes.

C. Employee Rights

You may have rights under California law to:

- Receive additional information regarding the Company's data practices;

- Request access to, correction of, or deletion of personal information, subject to statutory exemptions.

Nothing in this Agreement is intended to limit rights that cannot be waived under California law.

5. New York – Labor Law and Privacy Requirements

This section applies to individuals covered by New York Labor Law § 201-a and related privacy statutes.

The Company:

- Provides written notice of biometric data collection;
- Obtains written consent prior to collection;
- Uses biometric data solely for employment-related purposes;
- Implements reasonable safeguards to protect such data.

6. Colorado – Biometric Identifier and Biometric Data Requirements

This section applies to individuals covered by applicable Colorado biometric identifier and biometric data requirements.

The Company may collect, capture, store, use, process, or disclose Biometric Information only as described in this Agreement and only for the disclosed employment-related purposes, including timekeeping, payroll administration, identity verification, prevention of timekeeping fraud, jobsite access control, workplace safety, and compliance.

The Company will provide notice and obtain consent before collecting or processing biometric identifiers or biometric data where required by Colorado law. For Colorado employees, contractors, applicants, interns, fellows, or other covered individuals, the Company will not require consent to the collection or processing of biometric identifiers except as permitted by applicable law.

The Company will maintain a written biometric policy that establishes a retention schedule for biometric identifiers and biometric data, includes a protocol for responding to a data security incident that may compromise biometric identifiers or biometric data, and includes guidelines for deletion of biometric identifiers.

Where Colorado law applies, biometric identifiers will be deleted no later than the earliest of:

- (1) the date upon which the initial purpose for collecting the biometric identifier has been satisfied;
- (2) twenty-four (24) months after your last interaction with the Company; or
- (3) the earliest reasonably feasible date, not more than forty-five (45) days after the Company determines, following at least an annual review, that continued storage is no longer necessary,

adequate, or relevant to the disclosed processing purpose, subject to any extension permitted by applicable law.

Nothing in this Colorado section limits any rights that cannot be waived under applicable law.

7. Other States and Local Laws

If you work in a state or locality that enacts additional biometric privacy requirements, the Company will comply with such laws as applicable and may provide supplemental notices or obtain additional consent.

8. No Waiver of Non-Waivable Rights

Nothing in this Addendum or the Agreement is intended to waive any employee or worker rights that cannot legally be waived under applicable federal, state, or local law.

Acknowledgment

By signing the Agreement, you acknowledge receipt of this Addendum and confirm that you have read and understand the state-specific disclosures applicable to you.