UKG Device Finger and Face Scan Data Statement

November 2, 2022

Table of Contents

This Statement supersedes any previous statements or documentation, is for information purposes only, and it does not constitute legal advice or advice on how to achieve operational privacy and security. If you require legal advice on the requirements of the GDPR, or any other law, you are advised to consult a suitably qualified legal professional. If you require advice on the nature of the technical and organizational measures that are required to deliver operational privacy and security in your organization, you should consult a suitably qualified privacy and security professional. UKG believes that the information in this Statement is accurate as of the publication date. All information provided, including any specifications, is subject to change without notice.

Device Finger and Face Scan Data Statement

The privacy and information security landscape is dynamic and evolving. While finger and face scanning are robust and efficient security measures for timekeeping devices offered by UKG, there have been various legislative efforts aimed at regulating biometric data to ensure that the collection and use of it is for an appropriate purpose and/or done only with the individual's knowledge and consent.

All customers who use our finger or face scan devices must understand these evolving legal requirements and implement policies and procedures that ensure the adequate protection and compliant use of this data. In some jurisdictions, these policies and procedures should ensure that appropriate prior consents are obtained from individuals and expressly authorize the disclosure of this data to UKG in connection with the use of our timekeeping devices. In addition, there may be requirements concerning the protection, retention, and destruction of the data that customers are responsible for complying with.

In this Statement UKG is not providing legal or information security advice, nor acknowledging that any finger or face scan data from UKG devices constitutes biometric data in every jurisdiction. Customers must obtain their own legal guidance and information security advice and make their own decisions regarding how to achieve compliance with these laws in their use of our products. Finger or face scan data is customer data that is owned and controlled by the customer; it is subject to that customer's rules and policies and any related compliance with these laws is the customer's responsibility. As part of managing its responsibilities, customers are also encouraged to stay informed of the rapidly changing landscape regarding privacy laws related to biometrics.

UKG, as a vendor or service provider, does not control how UKG customers handle data of their own employees or personnel ("End Users"). Finger or face scan data may be collected or stored by UKG customers along with other End User data. With our devices, our customers have the ability to collect finger or face scan data and may store that data at a customer-controlled site or on secure space (in accordance with applicable law) made available by UKG in a cloud environment for that purpose. Any data customers store on a secure space made available by UKG is at all times customer data, which UKG cannot access except as permitted by contract or with customer consent. To the extent required by law, customers may need to obtain written authorization from each individual prior to the collection of this data, including prior to employee enrollment at the device. Certain timekeeping devices have "notice and consent" screens embedded into the device, which our customers can utilize to provide notice to and obtain consent from their own End Users. UKG makes available a copy of this "notice and consent" screen at UKG.com/noticeandconsent which can be printed and kept by customers and their End Users. Customers with previously enrolled End Users are encouraged to re-enroll End Users at applicable devices through the "notice and consent" screens.

Our timekeeping software will manage this data in accordance with the instructions provided by our customers and solely for our customer's timekeeping purposes. These products provide for a finger or facial scan technology option. Please note that alternative options are provided by UKG, and that customers are free to de-activate the finger or facial scan technology option. We do not sell, lease, or trade any customer finger or face scan data that is generated through our customer's use of those devices.

UKG's finger and face scan timekeeping devices do not store any actual fingerprints or facial images. The enrollment process performs a set of measurements of the finger or face scan. The data is converted at the

devices prior to storage by a proprietary algorithm into mathematical representations (encoding), known as a template, that cannot be reverse engineered into an individual's actual fingerprint or facial geometry. Moreover, UKG protects template data at rest in the device through encryption and/or encoding measures (depending on the type of device) and encodes and encrypts template data within its cloud environment, and while in transit from the devices to the cloud. Since templates are encrypted at the database level, we do not support a "bring your own keys" option for customers. We maintain our privacy and security programs in a manner that complies with our customer agreements. UKG's Data Processing Addendum describes our technical and organizational measures with respect to privacy and data security. UKG flagship cloud solutions comply with ISAE3402/SSAE 18 AICPA Trust Principles for Security, Confidentiality, Availability and, depending on the application, Processing Integrity and Privacy. Further, UKG's policies align with ISO 27001, 27017, and 27018 standards and, depending on the application, our solutions have achieved certification against these standards.

UKG has put reasonable measures in place to minimize its access to customer End User finger or face scan data, which would occur in limited situations such as for technical support. In those rare occasions, such access is only pursuant to the customer's agreement, subject to strict handling procedures, which may require de-identification, and is limited in duration.

UKG customers are responsible for timely destruction of customer End User finger and face scans that they collect, control, possess or store in accordance with applicable law, including without limitation, upon the initial purpose for collection of the templates by customer being satisfied, such as termination of an End User's employment with customer, an End User discontinuing use of UKG's finger or face scan technology, or the customer discontinuing use of UKG's finger or face scan timekeeping devices. UKG's finger or face scan timekeeping devices, and/or the web portal to the services (depending on the type of timekeeping device), allow UKG customers to define their own retention periods and delete the template data. At the termination of a customer's contract, UKG will delete the data in accordance with applicable contracts, laws, and any active legal proceedings (i.e., litigation hold). Any questions regarding customer finger or face scan End User templates, including any applicable retention schedule or destruction process, should be directed to the appropriate employer.

In addition, UKG has made available for information purposes only sample timekeeping policies for customers utilizing our UKG devices. These sample timekeeping policies do not constitute legal advice or advice on how to achieve operational privacy and security. Customers are encouraged to review and assess, in consultation with their own legal advisors, adopting their own timekeeping policy that addresses applicable compliance requirements.

For information regarding UKG's external website privacy notice, see also: UKG.com/privacy.

Product-Specific Information

InTouch - Finger and Face Scan

This Statement is intended to provide information for customers who deploy the UKG Touch ID, Touch ID Plus or TouchFree ID devices and choose to utilize the finger or facial scan option. This information may be used to inform the assessments our customers need to make under applicable laws related to biometrics.

Embedded Consent

For customers utilizing UKG Touch ID, Touch ID Plus or TouchFree ID devices outside North America, the embedded consent feature is optional, and our customers can choose to obtain consent through alternative means or may choose to use alternative means for End User authentication purposes. UKG makes available a copy of this "notice and consent" screen at UKG.com/noticeandconsent, which can be printed and kept by customers and their End Users.

Deletion

Finger scan and face scan templates can be deleted by the Touch ID, Touch ID Plus, and TouchFree ID user in the following ways:

1. Un-enroll the End User at a UKG InTouch or 4500 device. An authorized manager or supervisor can access manager mode at the device and perform an Unenroll employee transaction. The steps for template deletion are described in the applicable user guides. This process permanently deletes the finger scan or face scan stored on the Touch ID, Touch ID Plus, or TouchFree ID option at that device. The unenrollment is communicated to the UKG Dimensions, UKG Workforce Central, or UKG Ready server, and the templates for that End User are then permanently deleted from the server database. The unenrollment is also sent to other devices the End User was assigned to the next time an Initialize or Update with Employee template data is performed, and the finger scan or face scan templates for that End User are permanently deleted from the Touch ID, Touch ID Plus or TouchFree ID options installed at those devices as well.
2. Delete templates in the People Editor in UKG Dimensions, UKG Workforce Central or UKG Ready. An authorized manager or administrator can perform this task on a desktop system, either as part of the End User termination process or at any time if an End User will no longer use finger scan or face scan devices. This will permanently delete the templates from the server database, and the next time an Initialize or Update with Employee template data is performed, the templates for that End User are permanently deleted from the Touch ID, or Touch ID Plus, or TouchFree ID options installed at those devices as well. Please consult the user guides or online help for the applicable software application.
3. For recent versions of UKG software, specifically UKG Workforce Central versions 8.0 and 8.1, and current versions of UKG Dimensions and UKG Ready the Touch ID, Touch ID Plus, and TouchFree ID user can configure the system to automatically delete templates when an End User is terminated.

When used with earlier versions of UKG Workforce Central and all other UKG software, the templates are retained when an End User is marked Terminated to eliminate the need to reenroll the End User if they are marked Active again in the future. Templates for Terminated End Users must be deleted manually using one of the approaches described above. Alternatively, if requested, UKG Professional Services can provide customers with a database script that will delete templates for all End Users marked terminated.

To ensure deletion of all copies of the template data, any application database backups created by UKG Workforce Central On-Premise users prior to deletion of templates must be deleted and replaced with a new database backup. All UKG Workforce Central and Dimensions users should ensure that the "Purge Old Device Data Event" is enabled and is scheduled to run regularly to delete backup copies of template data (please refer to your product's documentation or online help for instructions). Database backups created prior to deletion of templates for UKG cloud users are deleted in accordance with the terms of our customer agreements and no longer than 1 year after the date the template is deleted from the application database by the customer.

Cross Border Transfers

UKG has put reasonable measures in place to minimize its access to customer End-User finger or face scan data, which would only occur in limited situations such as for technical support. In those rare occasions, such access is only pursuant to the customer's agreement, subject to strict handling procedures, which may require de-identification, and is limited in duration.

UKG provides support for customers using our cloud services in the following locations:

1) Australia
2) Canada
3) European Union
4) United Kingdom
5) United States

Our customers may choose to ship and install finger or face scan devices to other locations. UKG does not control where our customers ship or install finger or face scan devices after customers receive them from UKG. It is our customer's obligation to ensure that their use of the devices in such locations complies with applicable law.

UKG makes available a list of subprocessors, which contains for each subprocessor the applicable safeguards. The UKG Supplier Code of Conduct applies to all subprocessors, and where required, UKG includes cross-border mechanisms and/or supplemental measures to comply with applicable laws and regulations.

The data center hosting locations of customer data and the applicable security safeguards in place are listed below:

UKG Ready	Google Cloud Platform (GCP)	Google Inc. 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	For safeguards, please refer to UKG's SOC 2 report. Additional information about Google's safeguards are available on https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf
UKG Dimensions	Google Cloud Platform (GCP)	Google Inc. 1600 Amphitheatre Pky Mountain View, California 94043 USA	For safeguards, please refer to UKG's SOC 2 report. Additional information about Google's safeguards are available on https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf
UKG WFC	Cyxtera	Cyxtera Technologies, Inc. BAC Colonnade Office Towers 2333 Ponce De Leon Blvd, Suite 900 Coral Gables, FL 33134 USA	For safeguards, please refer to UKG's SOC 2 report. Additional information about Cyxtera's applicable safeguards are available on https://www.cyxtera.com/colocation-services/compliance
UKG WFC	Equinix	Equinix (Germany) GmbH Kleyerstraße 88-90, 60326 Frankfurt am Main, Germany and Equinix (Netherlands) B.V. Luttenbergweg 4. 1101 EC Amsterdam Zuidoost The Netherlands	For safeguards, please refer to UKG's SOC 2 report. Additional information about Equinix's applicable safeguards are available on https://www.equinix.com/data-centers/design/standards-compliance

The co-location providers listed above do not generally have access to customer data.

Frequently Asked Questions Regarding UKG finger and face scan Touch ID, and Touch ID Plus, and TouchFree ID Devices

Q. What are Touch ID, and Touch ID Plus, and TouchFree ID Devices?

A. These timekeeping devices are used to authenticate customer End Users of UKG devices via a finger scan or a face scan.

Q. What is the purpose of managing finger/face scans by UKG's timekeeping software?

A. Finger and face scans are used to authenticate customer End Users when entering or viewing time worked data, to help ensure that the proper user is entering or viewing the data.

Q. Are alternative means provided by UKG, which would be less intrusive but would however enable the use of the service?

A. UKG offers multiple options for customer End Users to authenticate at UKG timekeeping devices that do not require a finger or face scan. These methods include using an employer issued identification card or typing in an employer issued badge ID that is unique for each End User.

Q. Is the End User finger scan data created when using the UKG Touch ID and Touch ID Plus Devices a fingerprint?

A. The finger scan data generated from the UKG Touch ID and Touch ID Plus devices does not contain a fingerprint or image of any kind, but instead consists solely of templates with numbers created from mathematical algorithms which are protected through encryption and/or encoding measures (depending on the type of device). UKG does not control the finger scan data that is generated from the Touch ID and Touch ID Plus devices. For a legal definition of what is considered to be "based on" or derived from a fingerprint, please consult with your own legal counsel for interpretation and guidance with respect to the applicable laws.

Q. How is End User finger scan data created when using the UKG Touch ID and Touch IDPlus Devices?

A. End User finger scan data is created during the enrollment process at UKG 4500 or InTouch devices with the Touch ID or Touch ID Plus options installed. The enrollment process generates finger scan data that is immediately converted into a numerical template using a proprietary mathematical algorithm and which is protected through encryption and/or encoding measures (depending on the type of device) to protect against unauthorized access until such data is deleted within the system. No fingerprint is ever taken or stored, and no image of the finger, or image of any kind, is stored as part of the enrollment or verification process. The finger scan template generated by the UKG Touch ID or Touch ID Plus device consists solely of numerical data based on proprietary algorithms.

Q. How is End User face scan data created when using UKG TouchFree ID?

A. End User face scan data is created during the enrollment process at UKG InTouch devices with the TouchFree ID option installed. The enrollment process generates face scan data that is immediately converted into a numerical template using a proprietary mathematical algorithm and which is encrypted and encoded to protect against unauthorized access until such data is deleted within the system. The face scan template generated by the UKG TouchFree ID consists solely of numerical data based on proprietary algorithms.

Q. How are templates deleted? Can the Touch ID, Touch ID Plus, and TouchFree ID user configure the system to automatically delete templates when an employee is terminated?

A. Please refer to the "Deletion of finger and face scans" section earlier in this document.

Q. Does UKG sell, lease, trade, or otherwise profit from the finger scan data that is created by the Touch ID or Touch ID Plus devices or face scan data created by the TouchFree ID device?

A. No. UKG has a strict policy prohibiting the sale or renting of personal information, including finger and face scan data.

TouchBase – Face Scan

This Statement is intended to provide information for customers who deploy the UKG TouchBase devices and choose to utilize the face scan option. This information may be used to inform the assessments our customers need to make under applicable laws related to biometrics.

Background

UKG Pro Time Collection hardware (also known as "UTC Hardware" or "timeclock devices") provide the ability for customers to collect employee time/labor data used to populate employee timesheets within UKG Pro for payroll purposes. Certain devices include a built-in camera for the purpose of collecting photos of employee faces when employees perform Time & Attendance punches and other interactions at the time clock. The photo-taking capability can be enabled or disabled by customers on a "per clock" basis. Photos are stored in the clocks and in the UKG Pro Time Collection (UTC) Host server database which is hosted in UKG cloud. Customers may also elect to enable a "Buddy Punch Alert" feature which leverages a facial recognition comparison algorithm to validate an employee's identity and alert on punches where the employee face does not match prior photos of the same employee. For customers that enable this Buddy Punch Alert, the facial comparison feature is conducted offline at the UTC Host server (not in real time as the employee punches at the clock) and can be configured to run at specific days/times or at regular intervals.

Customer Photo Data

Customers enable/disable features such as taking photos and the facial comparison feature, at their sole discretion. Photo-taking can be enabled/disabled by customers via configuration setting on a per-clock basis. If photo-taking is enabled, the clock takes a photo of each employee's face immediately after they identify

themselves at the clock by inputting their badge/ID. Each employee has a chance to review his/her photo that will be tagged to the punch, prior to proceeding with the punch and has an option to cancel the punch and start the process again.

Optional Facial Recognition Buddy Punch Alert Feature

Customers decide whether or not to enable the facial comparison feature of the UKG Pro time clocks. This feature compares new punch photos to the stored training set photos of each employee. As further outlined below, any facial comparison information or data runs on the Host Server at regular intervals or pre-defined times. When the Facial Recognition analysis runs, it generates facial geometry data from the existing training set photos as well as from new punch photos of that employee and uses a facial recognition algorithm to flag any new punch photos that do not match that employee's training set. The facial geometry data is generated "on the fly" in server memory. After the analysis is complete, the generated facial geometry data is dropped from memory. The facial geometry data is never physically stored in a database, only the original punch photo images are stored. Therefore, neither clients nor UKG have ability to access or copy the facial geometry data created by the facial comparison feature.

In the event that there are punch photos flagged by the facial comparison feature process that are deemed not to match training photo set data of the same individual, an email alert will be automatically generated and sent from the UTC Host server to the customer's designated administrator or to the designated customer supervisor and contains the photo at issue. It is the customer's decision whether to take any follow up action in response to the suspected "Buddy Punch". There is no follow-up by UKG regarding any alert, and UKG has no knowledge of, and provides no recommendations regarding, what a customer may do following receipt of an alert. Because time punches will already have been posted to timesheets in UKG Pro, customers also bear the sole responsibility for correcting any time punches that the customer is unable to validate. This is an exception-based alert only and absent a customer's correction, UKG Pro's timekeeping and timesheet functions will assume that the time punches are correct.

Data Storage, Retention and Security

As a Software-as-a-Service (SaaS) provider, ensuring security of customer's employee data is a top priority. UKG takes substantial measures to safeguard any UKG provided storage environment for customers to store personal/sensitive information (for all UKG Pro products/applications), including photos and information described in this document. We maintain our privacy and security programs in a manner that complies with our customer agreements. UKG's Data Processing Addendum describes our technical and organizational measures with respect to privacy and data security.

By default, employee punch photos are retained in the clocks and UTC Host Server database for 30 days, unless clients elect a longer or shorter retention period. Retention for this limited time period allows authorized customer administrators sufficient time to review any past punches and photos for audit/review. After this period, the punch photos are deleted from the clocks and the host server. Photos are not stored, transmitted, or used outside of the clock itself and the UTC Host Server database. The only information sent to the UKG Pro Time system is the punch information (such as clock-in and clock-out dates and times) for each of the customer's

employees, which is used to populate the customer's timesheets for that employee. The punch photos are not sent to the UKG Pro Time system.

The only exception where employee punch photos will be retained for a longer period than described above is in the event that the optional Facial Recognition Buddy Punch Alert is enabled. In this case, the UTC Host server will store/maintain a set of 15-25 punch photos for each employee which are designated as "training set" photos that will be used as a baseline to compare new punch photos against. By default, the first 15-25 photos of each employee are marked as "training" photos. Subsequent to that, the customer has ability to replace any invalid training photos with newer photos to ensure that each of these training photos always represent a true likeness of the employee in order to yield accurate facial recognition results. The training photos are retained indefinitely on the host server until employee is terminated in UKG Pro or a request is made to remove the training set photos. In this case, they will be permanently removed from the UTC Host server within 30 days of the termination/request.

With the exception of Training photos used for facial recognition analysis as described above, photos are stored only for the customer configurable amount of time (usually 30 days after being collected, which is the default setting) and then purged or permanently destroyed. Photos may also be stored for up to 90 days as part of routine server host back-ups, as required for customer's business continuity purposes.

Photos of a customer's employees are not exported by UKG to other applications or third parties. Because customers own the data, customers with authorized administrative credentials can access and export their data such as punch reports and photos. Any third-party requests to UKG are subject to review by customer and require a valid subpoena or Court Order. Facial comparison data is not retained, is automatically deleted, and cannot be replicated.

TimeBase – Finger Scan

This Statement is intended to provide information for customers who deploy the UKG TimeBase devices and choose to utilize the finger scan option. This information may be used to inform the assessments our customers need to make under applicable laws related to biometrics.

Background

UKG Pro Time Collection hardware (also known as "UTC Hardware" or "time clock devices") provide the ability for customers to collect employee time/labor data used to populate employee timesheets within UKG Pro for payroll purposes. Customers have the option of ordering devices with or without a finger scan module. For device models with finger scan module, the scanner reads an employee's finger and extracts data points and patterns from the finger scan to create a mathematical representation ("template") which is used to validate the employee's identity when the employee performs Time & Attendance punches at the time clocks. Even if a customer orders and implements devices with a finger scan module, the finger scan

capability can be enabled or disabled by customers on a "per clock" basis. The templates are stored in the clocks and in the UKG Pro Time Collection (UTC) Host Server database.

Customer Finger Scan Data

Customers enable/disable features such as taking finger scans at their sole discretion. Finger scans can be enabled by customers on a per-clock basis and customers can exempt certain employees from needing to scan their finger, even if the clock is otherwise configured to prompt for other employee finger scans. Each employee who will be subject to finger scan validation needs to enroll/register their finger data prior to using the clock for the first time. This is a supervisor-led process where the employee will be prompted to input their badge number and then their scan finger on the device three times. The finger scan reader does not actually store a raw finger scan image. During the enrollment process, it captures key points and physical patterns from the surface finger as well as other subdermal markers. These data points are processed into a string of numbers referred to as a template using a mathematical algorithm that is proprietary to the device. The templates are stored on the TimeBase clock upon enrollment of each employee and a copy is uploaded to the UTC Host Server. The server then sends a copy of the template to all the other clocks belonging to the same client which the employee is assigned to use.

Data Storage, Retention and Security

As a Software-as-a-Service (SaaS) provider, ensuring security of customer's employee data is a top priority. UKG takes substantial measures to safeguard any UKG provided storage environment for customers to store personal/sensitive information (for all UKG Pro products/applications), including templates and information described in this document. Template data is encoded at rest in the device and is encoded and encrypted within UKG's cloud environment, and while in transit from the devices to the cloud. We maintain our privacy and security programs in a manner that complies with our customer agreements. UKG's Data Processing Addendum describes our technical and organizational measures with respect to privacy and data security.

Templates are not stored, transmitted, or used outside of the clock itself and the UTC Host Server database. The only information sent to the UKG Pro Time system is the punch information (such as clock-in and clock-out dates and times) for each of the customer's employees, which is used to populate the customer's timesheets for that employee. The system does not have the capability to reverse engineer the template into an image or other form which would allow a human or other systems to interpret the finger scan data. Templates are retained in the clocks and database for the duration of the employee's employment and deleted within 30 days of an employee's termination or upon request by authorized client administrator. On occasion, back-up servers store copies of templates as part of routine back-up processes. In no event will templates be retained longer than 90 days after an employee's termination, after which time templates will be permanently destroyed.

Customer's employee finger scan templates are not exported by UKG to other applications or third parties. Because customers own the data, customers with authorized administrative credentials can access and export their data such as punch reports of customer's employees. Any third party requests are subject to review by customer and require a valid subpoena or Court Order.

Technical and Organizational Measures

InTouch and TouchBase

For the timekeeping devices that UKG has announced end of engineering support, UKG cannot guarantee that the ongoing security practices are in effect. For the timekeeping devices that UKG has not announced end of engineering support, the following technical and organizational measures apply:

- All UKG software engineers undergo annual training in the industry secure application development practices. All software architects receive additional training for their role.
- UKG has software security architects and a security focused task force comprised of several members from each product team.
- Secure design is incorporated into the architectural review process, which include:
    - threat/security risk modeling and mitigation
    - secure design review
    - secure code reviews
- UKG engineering uses a mix of dynamic and static code analysis tools
- Annual third party penetrating testing is conducted using the latest firmware at the time of testing, looking at items such as:
    - System Configuration and Hardening
    - Securing of Data at Rest and in Transit
    - Business Logic Flaws
    - Authentication and Authorization Flaws
    - Physical security of the device to tampering
    - Denial of Service

TimeBase

UKG has announced end of engineering support for its TimeBase devices. The following general technical and organizational measures apply:

- All UKG software engineers undergo annual training in the industry secure application development practices. All software architects receive additional training for their role.
- UKG has software security architects and a security focused task force comprised of several

members from each product team.

- Secure design is incorporated into the architectural review process, which include:
    - threat/security risk modeling and mitigation
    - secure design review
    - secure code reviews
- UKG engineering uses a mix of dynamic and static code analysis tools.

Sample Timekeeping Policies

UKG has made available for information purposes only sample timekeeping policies for customers utilizing our UKG devices. These sample timekeeping policies do not constitute legal advice or advice on how to achieve operational privacy and security. Customers are encouraged to review and assess, in consultation with their own legal advisors, adopting their own timekeeping policy that addresses applicable compliance requirements.

InTouch – Sample Timekeeping Policy

EMPLOYEE TIMEKEEPING POLICY AND WRITTEN RELEASE

1. **Purpose.**

   _____ (the "**Employer**") has instituted this Employee Timekeeping Policy to define the policy and procedures for its collection, storage, disclosure, use, protection, transmission, and destruction of the data provided by employees using the Employer's timeclocks and finger scan or face scan devices. Photo, finger scan or face scan data (collectively, the "**Data**") is provided by employees for the Employer's timekeeping purposes, to ensure employees are accurately paid for time worked through the Employer's payroll.

   It is the Employer's policy to ensure that this Data is used and handled in accordance with applicable data privacy laws, which may consider this Data to be biometric data, including the Illinois Biometric Information Privacy Act ("BIPA").

2. **Scope.**

   This Policy applies to the Employer's facilities throughout the United States, including but not limited to the State of Illinois, and all employees using photo, finger scan or face scan devices in those locations.

3. **Finger Scan and Face Scan Data.**

As part of the timekeeping process, the Employer uses timeclocks and software, equipped with photo, finger scan, or face scan capabilities, purchased from its third-party vendor, UKG Inc. or an affiliate, subsidiary, or related company of UKG ("UKG Company") (collectively, "**UKG**"), or from a reseller of UKG. The devices collect photos and/or scans of employee's fingers or faces, to verify that an employee is "clocking in" or "clocking out." The purpose of these collections is to ensure that employees are recognized and paid for their time worked. The finger scan and face scan devices use a secure technology that generates an encoded mathematical representation called a template or otherwise protected information. The Employer securely stores these templates for the duration of employment, within the timeclock devices on its own premises or on secure space made available by UKG in a cloud environment for that purpose.

Once employment ends, any stored Data (including photographs) will be permanently destroyed by the Employer within 90 days.[1] The Employer is responsible for data destruction. For information regarding the Employer's retention schedule and guidelines for permanently destroying the Data, please see the Employer's policy on its website at https://www._____.com/privacy-policy. The templates from the finger or face scans cannot be converted into an employee's actual fingerprints or an original image of the employee's face, respectively.

4. Written Release.

The Employer requires employees, as a condition of initial or continued employment, to sign a written release or consent authorizing the Employer, UKG and any of their subcontractors, resellers, vendors, or successors to collect, capture, use, store, transmit, obtain, possess, disclose or re-disclose the Data for timekeeping purposes and related technical support and backup purposes. The form of written release is attached hereto as Exhibit A. UKG and its subcontractors, resellers, vendors, or successors can only access such Data pursuant to the Employer's instructions and authorization. Employees may revoke their consent at any time by notifying the Employer in writing that they will no longer be using the finger scan or face scan devices for clocking in or out. Employer will provide reasonable accommodations to those employees who refuse to consent to the collection and use of their Data as described in this policy. Employees who do not consent or who revoke their consent are not permitted to use the finger or face scan features of any UKG timekeeping device.

5. Use, Disclosure, Protection, Storage and Destruction of Finger Scan and Face Scan Data.

Employee Data will only be used for the purposes and related activities set forth in this Policy. The Employer will not sell, lease, trade, or otherwise profit from an employee's Data. The Employer will not disclose, re-disclose, provide access to or otherwise disseminate any Data outside of the terms of the Policy, unless:

- The employee or the employee's legally authorized representative provides consent to such disclosure;
- The disclosed Data completes a financial transaction requested or authorized by the employee or the employee's legally authorized representative;
- The disclosure 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.

The Employer will use the reasonable standards of care within its industry for any storage, transmittal, or protection from disclosure of all Data, and it will follow standards of care that are the same or greater than the standards of care that the Employer uses to protect other employee data.

Employer's vendors and contractors, including UKG, have publicly represented that they do not sell, lease, trade, or profit from such Data, and that they use reasonable standards of care within their industries for any storage, transmittal or protection from disclosure of any such Data. Please see UKG's external website

[1] Note to Employer: Please refer to your product documentation for specific instructions on destroying Data for terminated employees.

privacy notice at https://www.ukg.com/privacy

The Employer will ensure that its contractors, and any of their subcontractors, also comply with this Policy. Those groups include, but are not limited to, temporary staffing agency employees.

EXHIBIT A – WRITTEN RELEASE

As an employee of _____ ("the Employer"), I agree to use the photo feature and/or to scan my finger(s) or face on a scanning device, which was purchased by the Employer from UKG Inc. or an affiliate, subsidiary, or related company of UKG ("UKG Company") (collectively, "UKG"), or from a reseller of UKG, as part of the Employer's timekeeping process. I acknowledge that the device takes my photo and/or scans my finger or face and that if a scanning process is used, it creates a mathematical representation called a template or other protected information that is securely stored during my employment. I understand that, once my employment is terminated, any photo, finger scan or face scan data ("Data") will be permanently destroyed within 90 days. These templates and information are used by the Employer for verification and timekeeping functions. I have read and understand the Employer's Employee Timekeeping Policy regarding the use, retention, protection, and destruction of my Data. As a condition of my initial or continued employment, I voluntarily consent to the collection, capture, storage, access to, use, possession, obtaining of, purchase or acquisition of, receipt through trade, and/or disclosure, re-disclosure, or other dissemination of my Data by the Employer, UKG and any of their subcontractors, resellers, vendors, or successors in accordance with this Policy. My consent applies to each use of the scanning device, including past and future use. I provide this consent for purposes of ensuring compliance with the Illinois Biometric Information Privacy Act ("BIPA") and any other applicable privacy laws, which may consider the Data biometric data. I understand that I may revoke this consent at any time by notifying the Employer in writing. I understand that I am not permitted to use the finger scan or face scan of any UKG timekeeping device if I have not signed this consent, or if I have revoked this consent, and that any such use without consent/with revoked consent will be considered my consent.

_____ _____

Employee Signature Date

_____

Employee Printed Name

_____

Employee's work address

Do not implement this policy without seeking advice of counsel. UKG recommends Employer consult its own legal counsel on how to best comply with BIPA and any other applicable laws. Nothing herein constitutes legal advice. This document supersedes any previous statements or documentation. All information provided, including any specifications, is subject to change without notice.

TouchBase – Sample Timekeeping Policy

EMPLOYEE TIMEKEEPING POLICY AND WRITTEN RELEASE

As _____'s ("Employer") employee, I understand that the clock in and out process for my employer includes taking a photo of my face and may result in generation of facial geometry data from these photos in order to validate my identity using face scan technology. This Policy addresses the collection, storage, disclosure and permanent destruction of my photos and facial geometry data that may be generated and used for timekeeping purposes related to my job. This Policy is intended to comply with Illinois' Biometric Information Privacy Act and other similar legislation in other jurisdictions.

Employer purchases and uses UKG Pro time clocks sold by UKG Inc. or an affiliate, subsidiary, or related company of UKG ("UKG Company") (collectively, "**UKG**"), or from a reseller of UKG. I agree and understand that the UKG Pro time clock uses a built-in camera to take and collect a photo of my face. The UKG Pro technology may also conduct a facial comparison analysis based on my punch photos. Any facial geometry data generated during the facial comparison analysis is done so "on the fly" in server memory and then immediately deleted following the comparison. Facial geometry data is not stored or saved. Neither UKG nor Employer has access to any facial geometry data. The photos themselves may be stored in and used via the UKG Pro Time Collection (UTC) Host servers, databases and other time clock devices in use by my Employer and access to view these photos is restricted to authorized Employer Administrators and UKG Pro Support personnel.

Within ninety (90) days following the termination of the employment relationship, or within one year of an employee's last interaction with Employer, whichever occurs first, any photos relating to the employee are permanently destroyed, unless otherwise required by law or legal process to retain the photo.

Employer and UKG use the reasonable standards of care within their industries for any storage, transmittal or protection from disclosure of any employee photos that each may have access to or possess, in a manner that is the same as or more protective than the manner in which each stores, transmits and protects other confidential and sensitive information. Employer also uses reasonable care to protect the security, confidentiality and integrity of all employees' photos by and through enforcement of this policy.

Employer will not sell, lease, trade, or otherwise profit from my employee photos. UKG has represented to Employer that it will not sell, lease, trade or otherwise profit from my employee photos.

Employer [insert conditions where customer can disclose photos to third parties or post on customer websites, if exported]. UKG will not disclose photos to third parties absent Employer request or a valid warrant or subpoena.

WRITTEN RELEASE

As an employee of _____ ("Employer"), I agree to use the photo feature and/or to scan my face on a scanning device, which was purchased by the Employer from UKG Inc. or an affiliate, subsidiary, or related company of UKG ("UKG Company") (collectively, "UKG"), or from a reseller of UKG, as part of the Employer's timekeeping process. I acknowledge that the device takes my photo and/or scans my face and that if a facial comparison process is used, any facial geometry data generated during the facial comparison analysis is done so "on the fly" in server memory and then immediately deleted following the comparison. I understand that,

once my employment is terminated, any photographs will be permanently destroyed within 90 days. These employee photos, and/or any facial comparison data described above ("Data") are used by the Employer for verification and timekeeping functions. I have read and understand the Employer's Employee Timekeeping Policy regarding the use, retention, protection, and destruction of my Data. As a condition of my initial or continued employment, I voluntarily consent to the collection, capture, storage, access to, use, possession, obtaining of, purchase or acquisition of, receipt through trade, and/or disclosure, re-disclosure, or other dissemination of my Data by Employer, UKG and any of their subcontractors, resellers, vendors, or successors in accordance with this Policy. My consent applies to each use of the scanning device, including past and future use. I provide this consent for purposes of ensuring compliance with the Illinois Biometric Information Privacy Act ("BIPA") and any other applicable privacy laws, which may consider the Data biometric data. I understand that I may revoke this consent at any time by notifying the Employer in writing. I understand that I am not permitted to use the face scan of any UKG timekeeping device if I have not signed this consent, or if I have revoked this consent, and that any such use without consent/with revoked consent will be considered my consent.

_____ _____

Employee Signature Date

_____

Employee Printed Name

Do not implement this Policy without seeking advice of counsel. UKG strongly recommends Employer consult its own legal counsel on how to best comply with Illinois' Biometric Information Privacy Act and any other applicable laws. This document supersedes any previous statements or documentation, is for information purposes only and nothing herein constitutes legal advice or advice on how to achieve operational privacy and security. All information provided, including any specifications, is subject to change without notice.

TimeBase – Sample Timekeeping Policy

EMPLOYEE TIMEKEEPING POLICY AND WRITTEN RELEASE

As _____'s ("Employer") employee, I understand that the clock in and out process for Employer includes scanning my finger using technology provided by UKG Inc. or an affiliate, subsidiary, or related company of UKG ("UKG Company") (collectively, "**UKG**"), or from a reseller of UKG. This Policy addresses the collection, storage, disclosure and permanent destruction of finger scan data that may be collected and used for timekeeping purposes related to my job. This Policy is intended to comply with Illinois' Biometric Information Privacy Act and other similar legislation in other jurisdictions.

Employer purchases and uses UKG Pro time clocks sold by UKG. I agree and understand that the UKG Pro time clock uses finger scan technology to collect an encoded, mathematical representation of my finger scan ("employee scan data"), which may be stored in and used via the UKG Pro time clocks, servers and databases to validate my identity and track my work hours. All employee finger scan data is securely stored in an encoded format by the UKG Pro Time Collection system ("UTC System") and is not stored, transmitted, or used outside the UTC System.

Employee scan data is collected and may be stored in or used by the UTC System for the duration of my employment. Within ninety (90) days following the termination of the employment relationship, or within one year of an employee's last interaction with Employer, whichever occurs first, any employee scan data is permanently destroyed, unless otherwise required by law or legal process to retain the data.

Employer and UKG use the reasonable standards of care within their industries for any storage, transmittal or protection from disclosure of any employee scan data that each may have access to or possess, in a manner that is the same as or more protective than the manner in which each stores, transmits and protects other confidential and sensitive information. Employer also uses reasonable care to protect the security, confidentiality and integrity of all employees' employee scan data by and through enforcement of this policy.

Employer will not sell, lease, trade, or otherwise profit from my employee scan data. UKG has represented to Employer that it will not sell, lease, trade or otherwise profit from my employee scan data.

Other than as set forth herein, neither Employer nor UKG will disclose my employee scan data unless the disclosure:

A. Completes a financial transaction requested and authorized by me or my legally authorized representative, including timekeeping/payroll transactions described above;
B. Is required by state or federal law, or municipal ordinance;
C. Is required pursuant to a warrant or subpoena issued by a court of competent jurisdiction; or
D. Is expressly consented to by me.

WRITTEN RELEASE

As an employee of _____ ("Employer"), I agree to scan my finger(s) on a scanning device, which was purchased by the Employer from UKG Inc. or an affiliate, subsidiary, or related company of UKG ("UKG Company") (collectively, "UKG"), or from a reseller of UKG, as part of the Employer's timekeeping process. I acknowledge that the device scans my finger and creates a mathematical representation called a template or other protected information ("Data") that is securely stored during my employment. I understand that, once my employment is terminated, any Data will be permanently destroyed within 90 days. These templates and information are used by the Employer for verification and timekeeping functions. I have read and understand the Employer's Employee Timekeeping Policy regarding the use, retention, protection, and destruction of my Data. As a condition of my initial or continued employment, I voluntarily consent to the collection, capture, storage, access to, use, possession, obtaining of, purchase or acquisition of, receipt through trade, and/or disclosure, re-disclosure, or other dissemination of my Data by Employer, UKG and any of their subcontractors, resellers, vendors, or successors in accordance with this Policy. My consent applies to each use of the scanning device, including past and future use. I provide this consent for purposes of ensuring compliance with the Illinois Biometric Information Privacy Act ("BIPA") and any other applicable privacy laws, which may consider the Data biometric data. I understand that I may revoke this consent at any time by notifying the Employer in writing. I understand that I am not permitted to use the finger scan of any UKG timekeeping device if I have not signed this consent, or if I have revoked this consent, and that any such use without consent/with revoked consent will be considered my consent.

Employee Signature

Date

Employee Printed Name

Do not implement this Policy without seeking advice of counsel. UKG strongly recommends Employer consult its own legal counsel on how to best comply with Illinois' Biometric Information Privacy Act and any other applicable laws. This document supersedes any previous statements or documentation, is for information purposes only and nothing herein constitutes legal advice or advice on how to achieve operational privacy and security. All information provided, including any specifications, is subject to change without notice.