UKG Device Finger and Face Scan Data Statement

Last Updated: September 15, 2023

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. All information provided, including any specifications, is subject to change without notice.

Device Finger and Face Scan Data Overview

The privacy and information security landscape is dynamic and evolving. While finger, face, and hand scanning are robust and efficient security measures for timekeeping devices offered by UKG, an entity acquired by UKG, or a reseller/partner ("Devices"), 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 these 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 these 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, face, or hand photo or template data from these Devices ("Device Data") constitutes biometric data in any particular instance or 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. Device 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"). Device Data may be collected or stored by UKG customers along with other End User data. With these Devices, our customers have the ability to collect Device 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 UKG 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 these "notice and consent" screens in order to have their consents maintained electronically.

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, facial, or hand scan technology option. Please note that alternative options are provided by UKG, and that customers are free to de-activate the finger, facial, or hand scan technology option. We do not sell, lease, or trade any customer Device Data that is generated through our customer's use of those Devices.

The enrollment process for UKG finger or face Devices performs a set of measurements of the finger or face scan. The data is converted prior to storage at the Devices by an algorithm into mathematical representations (encoding), known as a template, that cannot be reverse engineered into an individual's actual fingerprint or facial geometry.   Moreover, template data is protected at rest in the Device through encryption and/or encoding measures (depending on the type of Device) and template data is encoded and encrypted within UKG's 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 template 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 template data 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 the applicable technology, or the customer discontinuing use of UKG's Devices. UKG's finger or face scan Devices, and/or the web portal to the services (depending on the type of 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 End User template data, including any applicable retention schedule or destruction process, should be directed to the appropriate employer.

Customers who utilize Devices without embedded "notice and consent" screen capability are encouraged to obtain written consent from their End Users which expressly authorizes disclosure of Device Data to UKG in connection with the use of these Devices. UKG has made available for information purposes only a sample timekeeping policy and release for customers utilizing our UKG Devices. This sample timekeeping policy does 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

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

UKG Dimensions, UKG Ready, and current versions of UKG Workforce Central all support embedded "notice and consent screens" for customers utilizing UKG Touch ID, Touch ID Plus or TouchFree ID Devices in a data hosting center made available by UKG. Customers are encouraged to use these screens at the Devices to provide notice to and capture the consents of their employees or personnel using these Devices. 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 may choose to disable the UKG Touch ID, Touch ID Plus and TouchFree ID options and use alternative means for End User authentication purposes.

Deletion

Finger and face 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 or face template 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 or face 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 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 template 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. While UKG resources may access the database in which encoded or encrypted templates are stored for cloud customers, the templates are encoded or encrypted and are not accessed by UKG resources unless directed by the customer to assist in migration of templates along with all other customer data when the customer is migrating from one UKG solution to another.

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

UKG does not control where our customers ship, install, or use finger or face Devices. Pursuant to customer's agreement with UKG it is our customer's obligation to ensure that their use of the Devices in any locations complies with applicable law.

UKG makes available a list of subprocessors, which contains for each subprocessor the applicable safeguards. The UKG Third Party 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:

Product	Hosting Provider	Hosting Location	Applicable Security Safeguards
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 InTouch finger and face 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 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 templates by UKG's timekeeping software?

A. Finger and face templates 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 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 template data created when using the UKG Touch ID and Touch ID Plus Devices a fingerprint?

A. The finger template 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 template 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 template data created when using the UKG Touch ID and Touch IDPlus Devices?

A. End User finger template 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 performs a set of measurements of the finger scan 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 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 template data created when using UKG TouchFree ID?

A. End User face template data is created during the enrollment process at UKG InTouch devices with the TouchFree ID option installed. The enrollment process performs a set of measurements of the face scan 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 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 InTouch “Deletion of finger and face templates” section above.

Q. Does UKG sell, lease, trade, or otherwise profit from the finger template data that is created by the Touch ID or Touch ID Plus Devices or face template 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 template data.

TouchBase – Face

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. Touchbase devices include a built-in camera for the purpose of confirming an employee face is detected (“face detection”) and taking photos of employee faces (“live preview”) when employees perform Time & Attendance punches and other interactions at the time clock. Live-preview can be enabled or disabled at customer direction on a “per clock” basis, and face detection can be enabled or disabled at customer direction on a per clock and/or a per employee basis (these features are enabled by default). If live-preview is enabled, photos are stored in the clocks and in the UKG Pro Time Collection (UTC) host server database which is hosted in the UKG cloud. If face detection is enabled, employees are not allowed to complete transactions at the clock without a face being detected.

Customers may also elect to enable/disable “Face Match” and “Buddy Punch Alert” features (these features are disabled by default) which can be used to match prior photos (“training photos”) taken during clock interactions with each new photo taken, and to send an email alert to a manager if the new photo does not match prior photos. The Face Match and Buddy Punch Alerts are conducted offline at the UTC Host server (not in real time as the employee uses the clock) and can be configured to run at specific days/times or at regular intervals. Face Match and Buddy Punch Alerts can only be used on clocks and/or employees that also have face detection enabled.

Customer Photo and Template Data

Customers decide whether to enable/disable features such as live preview, face detection, and Face Match. If live preview is enabled, the clock takes a photo immediately after employees identify themselves at the clock by inputting their badge/ID. Photos are stored temporarily on the clock until sent to the server with the timekeeping information and are then deleted from the clock within a configurable time period. Photos are stored on the UTC host server for a configurable time period, after which they are automatically deleted within a configurable time period (note that this excludes training photos, as described below).

If Face Match is enabled, the UTC host server creates a template using an algorithm from data points and patterns in the training photos. That template is compared to a similar template created for each new punch photo taken to determine if the new punch photo matches the training photos. Templates from training photos are created and stored on the UTC host server, and are retained until the employee is terminated or the template is deleted.

If Buddy Punch Alerts are enabled, if there are new punch photos flagged by the Face Match process that are deemed not to match the current template for an employee, 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, which 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

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 templates as 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.

As mentioned previously, photos are stored temporarily on the clock until sent to the UTC host server with the timekeeping information and are then deleted from the clock within a configurable time period (7 days by default). Photos are stored on the UTC host server for a configurable time, after which they are automatically deleted: 30 days by default, configurable to up to 90 days (this excludes the training photos, as described below). 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 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.

If Face Match is enabled, the UTC host server will store/maintain a set of 15-25 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 Face Match 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 Face Match analysis as described above, photos are stored only for the customer configurable amount of time (usually 30 days, which is the default setting) and then 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.

If Face Match is enabled, customer's employee photo templates are not exported, disseminated, or disclosed by UKG to other applications or third parties. Because customers own the data UKG cannot disclose photo templates to third parties.

Templates created from employee photos are stored in encoded format and used only on the UTC host server. The system does not have the capability to reverse engineer the template into an image or other form. Templates are retained on the UTC host server (located outside Illinois) for the duration of the employee's employment and deleted within 30 days of an employee's termination or deletion or upon request by authorized client administrator. On occasion, back-up servers (located outside Illinois) 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 or deletion, after which time templates will be permanently destroyed.

TouchBase and TimeBase – Finger

This Statement is intended to provide information for customers who deploy the UKG TouchBase and 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 creates a mathematical representation ("template") from data points and patterns in the finger scan 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 Template 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 a portion of the fingertip. 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 TouchBase or 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

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. 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 templates are not exported, disseminated, or disclosed by UKG to other applications or third parties. Because customers own the data, UKG cannot disclose finger templates to third parties.

Technical and Organizational Measures

InTouch and TouchBase

For the Devices that UKG has announced end of engineering support, UKG cannot guarantee that the ongoing security practices are in effect. For the 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 includes:
  - 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 penetration 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 includes:
  - threat/security risk modeling and mitigation
  - secure design review
  - secure code reviews
- UKG engineering uses a mix of dynamic and static code analysis tools.

UKG Ready - Finger and Hand Devices

In connection with UKG Ready products/applications, finger or hand template data may be collected or stored by certain customers who utilize Devices with finger or hand scan technology that have been supplied by UKG, an entity acquired by UKG, or a reseller/partner. These customers may store finger or hand template data on a secure space (in accordance with applicable law) made available by UKG in a cloud environment for that purpose. The data protection principles in this Statement also apply to these finger and hand End User templates, including UKG's safeguards for network and data security. In addition, UKG's "notice and consent" language (see UKG.com/noticeandconsent) is available to these customers through the UKG Ready User Interface or a URL. UKG Ready also allows these customers to define their own retention periods and delete the template data by providing customers the ability to: 1) manually delete templates from the employee profile through UKG Ready or at the Device (depending upon model); and 2) configure the system to automatically delete templates when an End User is terminated. Any questions regarding these customer finger or hand End User templates, including any applicable retention schedule or destruction process, should be directed to the appropriate employer.

Sample Timekeeping Policy

Customers who utilize Devices without embedded “notice and consent” screen capability are encouraged to obtain written consent from their End Users which expressly authorizes disclosure of Device Data to UKG in connection with the use of these Devices. UKG has made available for information purposes only a sample timekeeping policy and release for customers utilizing our UKG Devices. This sample timekeeping policy does 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.

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 template or face template 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 located in [INSERT], 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 templates 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 or host server (depending on the type of device) use a secure technology that generates an encoded mathematical representation called a template. 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 finger or face templates 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 Template and Face Template 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

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

UKG.com/noticeandconsent

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. By signing below, I acknowledge and agree to the following:

- That the device takes my photo and/or scans my finger or face and that if a scanning process is used, the device or the host server (depending on the type of device) creates a mathematical representation called a template that is securely stored in the device and/or my Employer's timekeeping database during my employment.
- I understand that, once my employment is terminated, any photo, finger template or face template data ("Data") will be permanently destroyed within 90 days. This Data is used by the Employer for verification and timekeeping functions.
- That this Data may be considered biometric data.
- I understand that, where applicable, Employer is responsible for providing me with all notices and policies relating to use of my personal information, including but not limited to providing a description of the data usage and level of protection.
- I have read and understand the Employer's Employee Timekeeping Policy regarding the use, retention, protection, and distribution of my Data.
- As a condition of my initial or continued employment, I voluntarily consent (if permissible by applicable law) to the collection, capture, storage, access to, use, possession, dissemination, disclosure, re-disclosure, and hosting of my Data by the Employer, and UKG and any of their subcontractors, resellers, vendors, or successors in accordance with this Policy.
- That my consent applies to each use of the face camera and face scan software and/or finger sensor, including past and future use.
- That UKG processes personal information on behalf of my employer (more information is available at UKG.com/noticeandconsent).
- That I can contact Employer about any rights I may have in connection with my personal information, including any right to withdraw consent.
- 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.