# Biometric Timekeeping Privacy and Retention Policy

Voluntary finger scan timekeeping within PLA and its operating companies

| | |
|---|---|
| **Policy ID: HR-45-N2** | **Library revision: 2.0** |
| **Owner: Human Resources** | **Language: English** |
| **Revision date: November 16, 2026** | **Effective: Upon public posting and issuance to affected workers** |
| **Status: Approved** | **Continuity: Existing rights remain in effect**<br>**Supersedes HR-45-N2 and HR-45-F1, Library revision 1.0 (October 24, 2026).** |

## 1. Purpose and scope

PLA and its operating companies (the Company) protect biometric identifiers and information used to identify a person. A mathematical template derived from a finger scan is protected biometric information even when no fingerprint image is retained. This policy covers anyone whose biometric information the Company collects or controls, including an agency worker or contractor; it does not authorize enrolling any additional worker or group.

The authorized program is limited to voluntary finger scan identity verification for recording time accurately through the approved ADP timekeeping system and its identified providers. The authorized program must not retain fingerprint images. HR and the system owner must verify actual scan processing and deletion for the reader and disclose it before enrollment. Facial recognition, voiceprints, iris or retina scans, other biometric systems, and new purposes require separate review and authorization before collection. Ordinary badge, PIN, web clock or geofence functions do not establish that biometric information is collected.

## 2. How and where the program operates

At an approved site, the reader measures points from a finger during enrollment and creates a mathematical template. A later scan is compared with that template to verify the person making a time entry. The precise reader, matching mode, template storage, transfers and recipients must be verified for that site and described in the notice before enrollment. Treat templates on clocks, in central systems and with service providers as protected information.

HR and the timekeeping system owner must maintain a current site and device register showing the physical work address, legal employer, model and enabled feature, data collected, storage locations, providers, consent version, available alternative and deletion process. An equipment order, an enrollment instruction or the availability of an ADP feature is insufficient to establish current use. Do not enable a site or materially change its program until these controls and the applicable state and local requirements are confirmed.

## 3. Voluntary choice and accurate pay

Providing biometric information is not required to obtain or retain employment. A person may decline without adverse employment action or withdraw consent at any time by notifying HR or the manager, submitting a written request, or using the same or a similarly simple electronic method offered for consent. Withdrawal must be as easy as giving consent. Managers must arrange the traditional paper timecard alternative promptly and must not pressure a person to enroll, scan additional fingers or retry after declining or withdrawing. A different nonbiometric option may be offered only after it is verified and communicated; the paper option remains available.

Record and pay all compensable time, including when a reader fails, enrollment is incomplete, the system is offline or consent is declined. Do not delay a time entry or wages because of a biometric issue. Do not charge the worker for employer requested enrollment.

## 4. Notice and informed consent before collection

Before collecting or obtaining biometric information, provide a complete, understandable written notice identifying the actual employer, worksite, information collected, specific purpose, storage and use, retention term, recipients and applicable rights. Give the person this policy and any applicable privacy notice. Complete HR-45-F1 with the actual program facts and obtain the informed written release or legally valid electronic consent before enrollment. Obtain any separately required permission for disclosure and renewed consent before a material new use.

Use the applicable ADP notice and consent feature as well as the Company's legally sufficient notice and release. Link the device decision to the notice version, delivery and actual choice. A general handbook acknowledgment, a blank form or an unexplained ACCEPT prompt is insufficient. If required consent is missing, refused or withdrawn, do not collect or continue biometric use. Apply the alternative. Make this retention and destruction policy publicly available wherever required, including Illinois; a restricted Teams or HR folder alone does not satisfy that requirement.

Existing enrollments. For each person enrolled before this revision was issued, HR must confirm within 60 days of issuance that a completed notice and a signed or legally valid electronic release covering the actual program are on file. In Illinois and Colorado, suspend biometric use for the person immediately until that confirmation is made. Elsewhere, if confirmation is not made within 60 days, offer HR-45-F1 and suspend biometric use until the person consents. If the person declines or does not respond, use the paper timecard and delete the template under Section 7. Do not request new consent where valid current evidence is already on file. A new release does not cure earlier collection; Legal decides any remediation for earlier periods.

## 5. Limited use sharing and protection

Use biometric information only for the disclosed identity and timekeeping purpose. Do not sell, lease, trade or otherwise profit from it, use it for advertising or model training, or disclose it for an unrelated purpose. Limit access to authorized personnel and identified service providers with a lawful need. Contracts must address purpose limits, confidentiality, safeguards, subprocessors, incidents and timely permanent deletion. A contract alone does not authorize a disclosure.

Disclose or redisclose information only under a ground permitted by the applicable biometric law and after obtaining required consent. In Texas, Business and Commerce Code 503.001(c) allows disclosure only on the grounds it lists, and consent alone is not one of them. The Company's position is that ADP and other identified providers store and process templates only as the Company's service providers, under written contract, for the Company's own timekeeping purpose, and do not receive them for their own use. Legal must document that position and the supporting contract terms. Do not provide Texas biometric information to any other person unless Legal confirms a ground listed in 503.001(c). Use at least reasonable industry care and safeguards at least as protective as those used for other confidential and sensitive information. Require appropriate encryption, access controls and secure transmission, verify actual configurations, and do not email biometric templates or place them in personnel files or general Teams folders.

## 6. Retention and permanent destruction

Retain biometric information only while the disclosed purpose continues. Permanently destroy it without delay when the purpose is satisfied, including employment or the relevant assignment ending, transfer to work without biometric use, discontinuing the program or an effective withdrawal ending the purpose. Destroy it no later than three years after the person's last interaction with the Company, or sooner when applicable law requires. For information collected in Illinois, the only exception to these deadlines is a valid warrant or subpoena issued by a court of competent jurisdiction. Elsewhere, an exception applies only when Legal confirms in writing the specific law or court order that requires longer retention and the date that requirement ends. Do not use a general personnel record retention period for biometric templates.

For Colorado, also apply the earlier statutory destruction triggers and annual review stated below. The end of the authorized purpose remains the Company's earlier rule. Keep only the minimum separate lawful evidence of notice, consent, withdrawal and completed destruction under the applicable records schedule; do not keep the biometric identifier as proof of compliance.

## 7. ADP and other custodian deletion

HR must promptly notify the system owner when a destruction trigger occurs. The owner must stop biometric use, arrange the alternative if needed, request permanent deletion from ADP and all applicable vendors, remove the templates from every

relevant clock and central system, and verify completion. Document the trigger, request, affected systems and confirmation without retaining the template.

Do not assume an HR termination, disabled badge, removed application access or an Accepted consent status proves template deletion. Verify the actual product's automatic and manual deletion behavior, device synchronization and any backup copies. ADP's timekeeping retention terms do not replace the Company's earlier legal or policy deadlines. If an asserted preservation duty conflicts with destruction, HR or Legal must determine the exact lawful exception and deadline. In Illinois, only a valid warrant or subpoena issued by a court of competent jurisdiction delays destruction. A general legal hold does not permit indefinite biometric retention.

## 8. State and local requirements

Determine applicable law from actual work and collection locations and other legally relevant connections, including residency and where information is processed or disclosed. Include remote work and applicable city rules. Illinois requires a public retention policy and informed written release before collection, with destruction when the initial purpose is satisfied or within three years of last interaction, whichever occurs first. Its electronic signature provision does not eliminate notice or consent duties.

Colorado requires a written policy, incident response process, annual necessity review, advance notice and consent for covered employee biometric collection. Its destruction deadline is the earliest of purpose satisfaction, 24 months after the person's last interaction, or the earliest reasonably feasible date within 45 days after an annual or more frequent review determines retention is no longer necessary, adequate or relevant to the disclosed purpose. A specific statutory extension of that review based deadline does not extend an earlier purpose end or last interaction deadline. Disclose the actual category, purpose, retention period and sharing; apply the additional disclosure consent rules and employment purpose restrictions. The Company's voluntary choice applies even where a narrow statute would allow a requirement.

Texas requires notice and consent before commercial capture and generally requires destruction within a reasonable time, no later than one year after the purpose expires, subject to its specific exceptions. Our earlier purpose end rule applies. New York prohibits requiring employee fingerprinting as a condition of obtaining or keeping employment, except as provided by law. California restricts detrimental third party furnishing of employee fingerprints and, where the CCPA applies, requires notice at collection and applicable privacy rights. Apply Washington's specific statutory scope and exceptions rather than assuming a blanket exemption for employees. Consent never cures a prohibited use.

## 9. Incidents questions and protected rights

Report suspected loss, unauthorized access or disclosure promptly to HR and the applicable IT or security channel. Authorized responders must contain the incident, assess its scope and impact, and coordinate required notices. Notify affected individuals and authorities as required without unreasonable delay and no later than 30 days after discovery, applying any shorter legal deadline and only a specifically permitted delay. Permanently delete compromised identifiers from affected systems unless a specific lawful retention duty applies; HR or Legal must reconcile that duty with mandatory destruction and document the decision.

Contact HR or the manager for the current notice, a policy copy, the paper timecard option or help withdrawing consent or submitting a privacy request. Report It and other protected reporting routes remain available. The Company prohibits retaliation for declining, withdrawing or exercising a protected right. This policy does not waive legal rights or amend a separate executed agreement. Apply HR-18, HR-45 and HR-46 together with this policy and the applicable current law.