

# Privacy Policy

## Phiro JJS

Last Updated: 26 June 2026

### 1. Introduction

This Privacy Policy explains how Phiro JJS collects, uses, stores, discloses, and protects personal information when authorized users access or use the Phiro JJS mobile application, web portal, and related services.

Phiro JJS is an enterprise Human Capital Management System / HRIS application used by companies and their authorized users to manage employee self-service, attendance, approval workflows, HR administration, activity checkpoints, evidence-based activity records, notifications, and workforce management functions.

For the purpose of this Privacy Policy, “Phiro JJS,” “we,” “our,” or “us” refers to PT Spasi Indonesia as the provider and operator of the Phiro JJS platform. “Client Company” refers to the employer, organization, or enterprise customer that uses Phiro JJS. “User” refers to an individual authorized to use Phiro JJS through a Client Company.

### 2. Enterprise Service and Role of the Client Company

Phiro JJS is provided primarily as a business-to-business enterprise service. The Client Company determines user access, HR configuration, workflow configuration, attendance rules, checkpoint rules, retention requirements, and authorized administrators for its users.

Phiro JJS processes personal information to provide, maintain, secure, and support the platform in accordance with the configuration, agreement, and instructions of the relevant Client Company.

For employment-related data requests, users may need to contact their HR department or authorized administrator. Users may also contact us using the privacy/support contact listed in this Privacy Policy.

### 3. Information We Collect

Depending on the features enabled by the Client Company and the permissions granted by the user, Phiro JJS may collect the following categories of information:

| Data Category                    | Examples                                                                                                                                                                                                                                                                                       |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account and Identity Information | Name, employee ID, username, email address, phone number, company, department, job title, branch/work location, role, and access permission.                                                                                                                                                   |
| Employment and HR Information    | Organization structure, employment status, work schedule, shift, leave balance, HR request history, approval history, and related HR records configured by the Client Company.                                                                                                                 |
| Attendance Information           | Clock-in and clock-out time, attendance status, attendance method, schedule data, attendance location, geofence validation result if enabled, and attendance audit trail.                                                                                                                      |
| Location Data                    | Location data used for attendance validation, geofencing, checkpoint validation, audit trail, and misuse prevention. Location is collected for user-initiated location-based actions such as attendance or checkpoint submission, unless a future feature is separately disclosed and enabled. |

| Data Category                           | Examples                                                                                                                                                                                |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Activity Checkpoint Data                | Checkpoint submission time, checkpoint location, activity status, notes, evidence photo, and audit trail. This is checkpoint-based activity evidence, not continuous movement tracking. |
| Evidence Photos and Attachments         | Photos, images, files, or documents uploaded by users for attendance, activity checkpoint, HR request, supporting evidence, or related workflows.                                       |
| Device, Log, and Diagnostic Information | Device type, operating system, app version, IP address, device identifier, login activity, security logs, crash logs, diagnostic data, and system activity logs.                        |
| Notification and Support Information    | Push notification token, notification preferences, support messages, feedback, helpdesk communications, and related support records.                                                    |

## 4. Data Not Collected in the Mobile Application

The Phiro JJS mobile application does not run payroll processing and is not intended to collect or store BPJS, NPWP, payroll calculation, payslip, bank account, tax, or statutory contribution data. If any of these data types are introduced into the mobile application in the future, this Privacy Policy and the relevant Google Play Data Safety and Apple App Privacy disclosures must be updated before release.

Unless expressly disclosed in this Privacy Policy or a future update, Phiro JJS does not use the mobile application to collect contact lists, SMS, call logs, microphone recordings, payment card data, or advertising data for third-party advertising purposes.

## 5. How We Collect Information

- Directly from users when they log in, submit attendance, upload evidence photos, submit activity checkpoints, or complete HR workflows.
- From the Client Company or authorized HR administrator.
- From system configuration set by the Client Company.
- From device permissions granted by the user, including camera, location, notification, and file/photo permissions where applicable.
- From automatic logs generated when users access or use Phiro JJS.
- From support, feedback, or communication channels.

## 6. How We Use Information

- To provide HCMS, HRIS, attendance, approval, employee self-service, activity checkpoint, and workforce management functionality.
- To authenticate users and manage role-based access rights.
- To support attendance, shift, leave, overtime, HR request, approval, and workforce administration processes.
- To enable activity checkpoints, evidence review, reporting, and audit trails.
- To verify attendance or checkpoint submissions using location, geofencing, or evidence photos if enabled by the Client Company.
- To send push notifications, reminders, approval alerts, checkpoint/task notifications, and system messages.
- To maintain security, fraud prevention, misuse prevention, troubleshooting, auditability, and service reliability.

- To comply with contractual, legal, regulatory, audit, employment-related, or Client Company obligations.

## 7. Device Permissions

| Permission               | Purpose                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Camera                   | Used for evidence photo capture if enabled.                                                                                                                                                  |
| Location                 | Used for attendance location validation, geofencing, and activity checkpoint validation. Location is used for checkpoint-based actions and is not intended for continuous movement tracking. |
| Notifications            | Used to send HR alerts, approval notifications, reminders, checkpoint/task notifications, and system messages.                                                                               |
| Files / Photos / Storage | Used to upload documents, images, evidence photos, or attachments if enabled.                                                                                                                |
| Device Information       | Used for security, audit trail, diagnostics, fraud prevention, misuse prevention, and troubleshooting.                                                                                       |

Users may disable device permissions through their device settings. However, disabling required permissions may prevent users from using attendance, geofencing, evidence photo, or activity checkpoint features required by the Client Company.

## 8. No Face Recognition or Biometric Data Collection

Phiro JJS does not collect, process, store, or share any face data, facial templates, or biometric information. Our attendance and clock-in features rely strictly on Location Services (Geofencing) to verify user presence at the designated workspace. Any evidence photos captured through the app are stored strictly as visual attachments and are never subjected to facial recognition or any biometric scanning technologies.

## 9. Location Data, Geofencing, and Activity Checkpoints

Phiro JJS may collect location data when users perform attendance, geofencing, or activity checkpoint actions. Location data may be used to validate attendance location, confirm checkpoint location, support activity evidence, maintain history, support audit trail, and prevent misuse or unauthorized activity submission.

Phiro JJS activity tracking is checkpoint-based. The application records location and evidence only when a user performs or submits a relevant attendance action, activity checkpoint, or evidence-based HR activity. Phiro JJS is not designed to continuously track user movement or perform continuous background location tracking for activity monitoring under the current policy scope.

If a future version introduces background location or continuous tracking, we will update this Privacy Policy, store privacy disclosures, and in-app notices before enabling that feature.

## 10. Evidence Photos and Activity Records

Phiro JJS may allow users to submit evidence photos as part of activity tracking, field activity reporting, attendance support, or HR-related requests if the feature is enabled by the Client Company.

Evidence photos are collected only when the user takes or uploads a photo for a specific activity, checkpoint, request, or workflow. Evidence photos are used to support verification, accountability, approval, audit trail, and operational reporting. They are not used for advertising or cross-app tracking.

## 11. Basis for Processing

- User consent for permission-based features such as camera, location, notifications, and evidence photo submission, where applicable.
- The need to provide HR, attendance, approval, activity checkpoint, and workforce management services requested by the Client Company.
- Contractual obligations between the Client Company and Phiro JJS.
- Legal, regulatory, employment, audit, or compliance obligations.
- Legitimate operational, audit, and security interests, where applicable.
- Instructions or configuration provided by the Client Company.

## 12. Sharing and Disclosure of Information

We do not sell users' personal information for advertising purposes.

We may disclose or make personal information available to authorized HR administrators, managers, approvers, supervisors, Client Company representatives, service providers supporting the platform, professional advisors, auditors, regulators, authorities, or successors where necessary for service delivery, security, compliance, legal obligation, audit, or business continuity.

We do not use attendance location data, activity checkpoint location, evidence photos, or HR records for advertising or cross-app tracking.

Where we use service providers or third-party processors, we require them to handle personal information only for authorized purposes and to apply appropriate confidentiality, security, and data protection safeguards.

## 13. Third-Party Services and SDKs

Phiro JJS may use third-party services or software development kits to support app functionality, infrastructure, hosting, storage, security, authentication, diagnostics, crash reporting, maps/location services, evidence upload, and push notifications.

The actual third-party service and SDK list must match the production builds before completing Google Play Data Safety and Apple App Privacy forms.

| Function                      | Service / SDK            |
|-------------------------------|--------------------------|
| Push Notifications            | Firebase cloud messaging |
| Crash Reporting / Diagnostics | Sentry                   |
| Maps / Location Services      | Googlemap service        |

## 14. Cookies and Similar Technologies

The Phiro JJS mobile application may not use browser cookies in the same way as websites. If users access Phiro JJS through a web portal, cookies or similar technologies may be used for login sessions, authentication, security, user preferences, and technical analytics.

## 15. Data Retention and Deletion

We retain personal information for as long as necessary to provide Phiro JJS services, comply with legal or contractual obligations, resolve disputes, maintain audit records, support security, and fulfill HR, employment, or regulatory requirements.

Activity checkpoint records, checkpoint location data, and evidence photos may be retained as part of HR activity history, operational reporting, approval records, security records, or audit trails according to the Client Company configuration and applicable retention requirements.

Because Phiro JJS is an enterprise HR platform, users may need to submit deletion, correction, or access requests to their employer or authorized HR administrator. Users may also use the privacy/support contact listed in this Privacy Policy for assistance.

If Phiro JJS allows users to create an account directly within the mobile application, we will provide users to request account deletion and associated data deletion, subject to legitimate retention requirements such as security, fraud prevention, audit, legal, regulatory, or employment obligations.

## 16. Data Security

We implement reasonable administrative, technical, and organizational safeguards designed to protect personal information from unauthorized access, disclosure, alteration, misuse, loss, or destruction. These safeguards may include role-based access control, authentication, limited access to authorized personnel, audit logs, secure data transmission where applicable, system monitoring, security review, and confidentiality obligations.

However, no method of transmission or storage is completely secure. We cannot guarantee absolute security of information.

## 17. User Rights and Choices

Subject to applicable laws and Client Company policies, users may have the right to request access, correction, update, deletion, restriction, objection, withdrawal of consent for permission-based features, and information about how their data is processed.

Because Phiro JJS is used as an enterprise HR platform, some requests may need to be submitted to the user's employer or authorized HR administrator. The Client Company may be responsible for handling employment-related data requests.

Users may withdraw device permissions through their device settings. Withdrawal of permissions may limit or prevent the use of certain features required by the Client Company, including attendance, geofencing, evidence photos, or activity checkpoints.

## 18. Children's Privacy

Phiro JJS is intended for enterprise workforce users and is not directed to children. We do not knowingly collect personal information from children for marketing or consumer purposes. If a Client Company authorizes a minor to use Phiro JJS in an employment, internship, or legally permitted workforce context, the Client Company is responsible for ensuring that such use complies with applicable laws and requirements.

## 19. International Transfer and Storage

Personal information may be stored or processed in Indonesia or other jurisdictions depending on the infrastructure, hosting arrangement, service provider, and Client Company configuration. Where required by applicable law, appropriate safeguards will be applied for cross-border transfer or processing of personal information.

## 20. Security Incident

If a security incident affects personal information, we will take appropriate steps to investigate, mitigate, and respond to the incident in accordance with applicable laws, contractual obligations, and internal procedures. Where required by applicable law or agreement, we will notify the relevant Client Company, users, authorities, or other affected parties.

## 21. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our services, legal requirements, security practices, or operational needs. When we update this Privacy Policy, we will revise the "Last Updated" date above. We may also notify users or Client Companies through the application, website, email, or other appropriate communication channels.

## 22. Contact Us

| Field                        | Information                                                                                                                                                               |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Company Name                 | PT Spasi Indonesia                                                                                                                                                        |
| Address                      | The Royal Palace, Jl. Prof. Dr. Soepomo, SH. 178 A Blok B No.29, RT.1/RW.15,<br>Menteng Dalam, Kec. Tebet, Kota Jakarta Selatan<br>Daerah Khusus Ibukota Jakarta<br>12870 |
| Support Email                | info@spasi.com                                                                                                                                                            |
| Website / Privacy Policy URL | <a href="https://phiraka.com">https://phiraka.com</a>                                                                                                                     |
| Application                  | Phiro JJS                                                                                                                                                                 |

For employment-related data requests, users may also contact their HR department or authorized administrator in their Client Company.