

Privacy Policy

yoram

This Privacy Policy explains how yoram (“Company”, “we”, “us”, or “our”) collects, uses, stores, shares, and protects personal data when users access or use the yoram mobile application, web platform, dashboards, and related services (collectively, the “Platform”).

By accessing or using the Platform, the user acknowledges that they have read and understood this Privacy Policy. Where required by applicable law, we will obtain the user’s consent before collecting or processing personal data.

1. Data Controller / Operator

The Platform is owned and operated by yoram, registered in the Kingdom of Saudi Arabia under its official registration, where applicable.

For privacy-related inquiries, users may contact us at the official contact channels available through the Platform.

2. Personal Data We May Collect

Depending on the user’s role and the services used, we may collect the following categories of personal data:

Account and identity information: name, username, ID or employee number, national ID or Iqama number where required, job title, company or organization name, and user role.

Contact information: email address, phone number, and communication preferences.

Profile information: profile photo, uploaded documents, permissions, assigned groups, office, department, or team.

Event and operational information: event name, location, schedule, tasks, checklists, incident reports, attendance, shift records, performance records, notes, and uploaded images or files.

Location and attendance data: location check-in/check-out information, QR scans, timestamps, and GPS-related data where enabled and required for operational purposes.

Device and technical data: device type, operating system, IP address, log data, app version, browser type, crash reports, and usage analytics.

Payment and billing data: subscription status, invoices, transaction references, and billing details. Card details or payment credentials should be processed by approved payment gateway providers and not stored by us unless expressly stated and legally permitted.

Support and communication data: messages, inquiries, complaints, feedback, and support tickets submitted through the Platform or by email.

3. How We Use Personal Data

We may process personal data for the following purposes:

Creating, verifying, managing, and securing user accounts.

Providing event operations services, including task management, team coordination, attendance tracking, reports, dashboards, and operational documentation.

Managing access levels, permissions, user groups, and organization accounts.

Providing customer support, troubleshooting, maintenance, and service improvements.

Sending service-related notifications, operational alerts, updates, and administrative messages.

Processing subscriptions, billing, invoices, and payment-related records.

Monitoring platform performance, preventing misuse, fraud, unauthorized access, or security incidents.

Complying with legal, regulatory, contractual, accounting, and audit requirements.

Improving the Platform, developing new features, and analyzing usage in an aggregated or anonymized manner where possible.

4. Legal Basis and Consent

We process personal data where necessary to provide the Platform, perform our contractual obligations, comply with legal requirements, protect legitimate operational and security interests, or where the user has provided consent. Where consent is required, the user may withdraw consent subject to applicable legal or contractual limitations.

5. Data Sharing and Disclosure

We do not sell personal data. We may share personal data only where necessary and in accordance with applicable law, including with:

The customer organization that created or manages the user account, such as the employer, event owner, office, or authorized administrator.

Authorized users within the same organization, according to their access level and permissions.

Service providers and processors who support hosting, cloud storage, analytics, notifications, customer support, cybersecurity, payment processing, or system maintenance.

Government authorities, regulators, courts, or law enforcement where disclosure is legally required or necessary to protect rights, safety, or security.

Professional advisers, auditors, insurers, or legal consultants where reasonably necessary for business, compliance, or dispute purposes.

A buyer, investor, or successor entity in the event of a merger, acquisition, restructuring, or transfer of the Platform, subject to appropriate confidentiality and data protection safeguards.

6. Data Retention

We retain personal data only for as long as reasonably necessary to provide the Platform, fulfill the purposes described in this Policy, comply with legal, accounting, audit, and contractual requirements, resolve disputes, and enforce our agreements. Retention periods may vary depending on the type of data, the customer's configuration, the nature of the event, and applicable legal requirements.

When personal data is no longer required, we will delete, anonymize, or securely archive it in accordance with our internal retention procedures and applicable law.

7. Security Measures

We use reasonable technical, organizational, and administrative measures designed to protect personal data against unauthorized access, loss, misuse, alteration, disclosure, or destruction. These measures may include access controls, authentication, encryption where appropriate, logging, backups, restricted permissions, and staff confidentiality controls.

No digital service can guarantee absolute security. Users must keep their login credentials confidential and immediately notify us if they suspect unauthorized access to their account.

8. User Rights

Subject to applicable law and verification of identity, users may have rights in relation to their personal data, including the right to request access, correction, completion, deletion, or restriction of processing, and the right to withdraw consent where processing is based on consent.

Requests may be submitted to the official contact channels available through the Platform. We may need to verify the request and coordinate with the customer organization that controls the relevant account or event data.

9. Location Data, Photos, and Operational Records

The Platform may use location data, photos, QR codes, attendance records, task logs, and timestamps to support event operations, staff coordination, security, attendance verification, performance monitoring, incident reporting, and audit trails. These features should be enabled only where necessary and authorized by the customer organization.

10. International Transfers

Some service providers, cloud infrastructure, or technical support providers may process or store data outside the Kingdom of Saudi Arabia. Where this occurs, we will apply appropriate safeguards and comply with applicable legal requirements relating to cross-border transfer of personal data.

11. Third-Party Services

The Platform may integrate with third-party services such as payment gateways, authentication providers, maps, analytics, cloud hosting, messaging, or government identity verification services. Use of those services may be subject to their own terms and privacy policies.

12. Children's Privacy

The Platform is intended for business and operational use and is not directed to individuals under the age of 18. We do not knowingly collect personal data from children under 18. If we become aware that such data has been collected without proper authorization, we will take reasonable steps to delete it.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. The updated version will be published through the Platform or otherwise made available to users. Where required, we will notify users or customer organizations of material changes.

14. Contact Us

For questions, requests, or complaints relating to this Privacy Policy or the processing of personal data, please contact:

Company: yoram

Contact: official contact channels available through the Platform