

pmo.one Privacy Policy

Version 1.0 · Effective [Oct 28, 2026]

This Privacy Policy explains what personal data pmo.one collects through the pmo.one website and platform, why we use it, who we share it with, and the choices you have.

Our commitments at a glance

- We never sell personal data.
- We do not use your data to train AI models.
- Uploaded contract files are processed in memory and are not stored.
- Data in your workspace is isolated from every other customer.
- You can access, correct, export or delete your personal data at any time.

1. Who we are and our role

Ehab Digital Marketing, Amman, Jordan operates pmo.one. Our role depends on the data:

Data	Our role	Who decides how it is used
Account, billing, website and support data	Controller	pmo.one, as described in this policy
Customer Data inside a workspace (projects, tasks, contracts metadata, resources, RAID items, and personal data within them)	Processor	The customer organization that owns the workspace

If you use pmo.one through your employer or a client, that organization controls the Customer Data in its workspace. Send requests about that data to your workspace Admin; we will help them respond. Our processing of Customer Data is also governed by our Terms of Use and Data Processing Addendum.

2. Data we collect

Category	Examples	Source
Account data	Name, work email, password (stored as a secure hash by Firebase Authentication), Google sign-in profile, role, workspace	You, your Admin, or Google if you use Google sign-in
Profile and resource data	Job title, department, skills and proficiency ratings, capacity, cost and billing rates, allocations, leave	You or your organization
Project and work data	Projects, tasks, assignments, comments, milestones, deliverables, sign-offs, risks and issues	You and other users in your workspace

Category	Examples	Source
Contract-derived data	Extracted parties, contact names, roles, milestones, clauses and financial terms	Contracts you upload (the files themselves are not stored)
AI Inputs and Outputs	Prompts to the AI Insights Copilot, generated briefings, suggested tasks, risk predictions	You and the AI Features
Usage and audit data	Sign-ins, actions, changed values, timestamps, IP address, device and browser type, AI token usage	Collected automatically
Billing data	Billing contact, company name, plan, invoices. Card details are handled by our payment provider, not stored by us	You
Communications	Support requests, feedback, emails to us	You
Website data	Pages visited, referrer, contact or demo-request form entries	You and cookies (Section 5)

We do not knowingly collect special-category data (such as health, biometric or religious data). Do not upload it unless your organization has a lawful basis and suitable safeguards.

3. How we use data and our legal bases

Purpose	Legal basis (where GDPR or similar laws apply)
Create and manage accounts, approve workspace access, enforce roles	Performance of a contract
Provide platform features, including dashboards, EVM, Monte Carlo, resource calendars and notifications	Performance of a contract
Run AI Features on your request (Section 4)	Performance of a contract
Keep audit logs, detect fraud and abuse, enforce our Terms and Google's Generative AI Prohibited Use Policy	Legitimate interests in security and compliance; legal obligation
Bill you and keep financial records	Performance of a contract; legal obligation
Respond to support requests	Performance of a contract; legitimate interests
Send service emails (approvals, password resets, assignment alerts)	Performance of a contract
Improve the platform using aggregated, de-	Legitimate interests

Purpose	Legal basis (where GDPR or similar laws apply)
identified usage statistics	
Send product news and marketing	Consent, which you can withdraw at any time

We do not sell personal data, use it for third-party advertising, or make decisions with legal or similarly significant effects about you based solely on automated processing.

4. AI processing and contract uploads

1. **When AI runs.** AI Features run only when a user triggers them, such as uploading a contract, generating tasks for a milestone, predicting risks, or asking the AI Insights Copilot a question.
2. **What is sent.** The relevant Input, and the workspace data needed to answer it, is sent from our servers to Google's Gemini API over encrypted connections. Your browser never calls Google's AI service directly.
3. **Contract files.** Uploaded files are held only in memory while Gemini extracts structured data, then discarded. They are not saved to cloud storage or disk. We keep only the extracted fields that a user reviews and approves.
4. **No training.** We do not use your data to train or fine-tune AI models. [Confirm your Gemini API terms and configuration also prevent Google from using prompts for training, and state Google's retention period for abuse monitoring.]
5. **Human oversight.** AI Outputs, including resource performance and skills insights, are suggestions for people to review. They are not used to make automated decisions about individuals.
6. **Acceptable use.** AI use is subject to [Google's Generative AI Prohibited Use Policy](#). Google may automatically screen requests for policy violations.

5. Cookies and similar technologies

Type	Purpose	Can you turn it off?
Strictly necessary	Keep you signed in (Firebase Authentication tokens in browser storage), protect against attacks, remember security settings	No; the platform cannot work without them
Preferences	Remember choices such as dashboard filters, view mode and theme	Yes, through your browser; some settings will reset

We do not use advertising or cross-site tracking cookies. Non-essential cookies are set only after you consent, where the law requires it.

6. Sharing and sub-processors

We share personal data only as needed to run pmo.one, and only with:

Recipient	Why	Data involved
-----------	-----	---------------

Recipient	Why	Data involved
Google Cloud / Firebase	Database hosting (Firestore), authentication, server infrastructure	All platform data
Google (Gemini API)	AI Features	AI Inputs and the workspace context needed for each request
Email delivery provider [e.g. EmailJS]	Approval, password-reset and notification emails	Name, email, message content
Payment processor [name]	Subscription billing	Billing contact and payment details
Other users in your workspace	Collaboration, according to their role	Your profile, assignments and activity
Professional advisers, authorities or courts	Legal compliance, defending legal claims	As required
A buyer or successor	Merger, acquisition or sale of assets, under this policy's protections	As needed

7. International transfers

Your data is hosted in United States multi-region. Our providers, including Google, may process data in other countries. Where data leaves the European Economic Area, the UK, or another region with transfer rules, we rely on adequacy decisions, Standard Contractual Clauses or equivalent safeguards required by local law.

8. Retention

Data	How long we keep it
Uploaded contract files	Not retained; discarded from memory once extraction finishes
Customer Data in a workspace	For the life of the subscription; deleted within 30 days after termination, unless the customer exports or asks us to delete it sooner
Deleted items (e.g. a deleted contract record)	Removed from the live database immediately
Account data	While your account is active; deleted or anonymized within 30 days of deactivation, unless your workspace keeps it for audit purposes
Audit logs	2 years, or longer where the law or the customer's

Data	How long we keep it
	compliance obligations require
Billing and tax records	As long as tax and accounting law requires, typically 2 years
Marketing preferences	Until you unsubscribe, plus a suppression record so we don't contact you again

9. Security

We protect personal data with technical and organizational measures, including:

- Encryption in transit (TLS/HTTPS) and at rest through our hosting provider.
- Strict tenant isolation: every record is tagged with its company ID and guarded by database security rules.
- Role- and plan-based access controls enforced in the app and in the database.
- AI and email credentials kept server-side, never in the browser.
- New users held in Pending Approval until a workspace Admin grants access.
- An immutable audit trail of sign-ins, permission changes and data changes.

If we become aware of a personal data breach affecting you, we will notify affected customers and authorities as the law requires. Report security concerns to info@pmo.one.

10. Your rights

Depending on where you live, you may have the right to:

- **Access** the personal data we hold about you and get a copy.
- **Correct** inaccurate or incomplete data.
- **Delete** your data, where we have no legal reason to keep it.
- **Export** your data in a portable, machine-readable format.
- **Restrict or object** to certain processing, including processing based on legitimate interests.
- **Withdraw consent** at any time, such as for marketing emails, without affecting earlier processing.
- **Complain** to your local data protection authority.

How to exercise them. Email info@pmo.one. We will verify your identity and respond within 30 days, or sooner if your local law requires. If your request concerns Customer Data in an organization's workspace, we will forward it to that organization's Admin, who decides how to respond. We will not discriminate against you for exercising your rights.

You can also update your profile directly in [pmo.one](#), and unsubscribe from marketing emails using the link in any message.

11. Children, changes and contact

Children. pmo.one is a business tool for people aged 18 and over. We do not knowingly collect data from children. If you believe a child has given us personal data, contact us and we will delete it.

Changes. We may update this policy as our services or the law change. We will post the new version here with a new effective date and, for material changes, notify workspace Admins in-app or by email at least 30 days in advance.

Contact. Ehab Digital Marketing, Amma, Jordan. Privacy questions and requests: info@pmo.one.