



AVIAD GOZ AI COACH



FAQ Security Related Questions

1. Employee Consent Process

Employees must accept the Terms of Use and Privacy Policy before accessing the platform. This provides formal consent and authorizes data processing.

2. Data Storage & Retention

All user interactions are processed and stored securely in our cloud environment.

Data is retained only for as long as the account is active, and thereafter only as required by law or to meet operational or dispute-resolution needs.

2a. Detailed Data Retention periods

Marga AI retains personal data for the duration that an End User account remains active, unless an earlier deletion is requested by the Master or End User.

The following categories apply:

- **Identification Data (name and email, where provided):**
Retained for the lifetime of the active account for account management, authentication, and billing administration.
Certain billing and transactional records may be retained for up to 7 years where required by applicable tax and accounting laws. Such retained data is isolated and not used for any other purpose.
 - **Conversation History (raw chat logs):**
Retained for the lifetime of the active account to enable access to prior interactions and ensure service continuity.
 - **Processed / Summarized Conversation Data:**
Retained for the lifetime of the active account to enable contextual, personalized AI guidance.
- All categories of data are encrypted at rest.

2b. Data Deletion Process

Upon account closure or upon written request by the Customer or End User, personal data will be deleted or destroyed within 30 days, except where retention is required by applicable law.

Where statutory retention obligations apply (e.g., financial recordkeeping requirements), the relevant data will be



retained only for the legally mandated period and will not be used for any additional processing purposes. Written confirmation of deletion can be provided upon request.

3. Document Uploads

Document uploads are not yet supported.

This feature is planned for a future release, at which point uploaded files will be protected with the same enterprise-grade security and encryption as all other data.

4. Certifications (ISO/IEC 27001, SOC 2, etc.)

We are in the process of ISO/IEC 27001 certification, confirming that our security controls and processes meet global standards.

5. Compliance with Regulations (GDPR, DPDPA)

We are progressing toward compliance and certification under GDPR, and will complete DPDPA compliance before deployment in India.

Our approach is designed to meet both global and local data protection requirements.

6. Encryption in Transit & At Rest

- Data in transit: encrypted using TLS
- Data at rest: encrypted using AES-256

These mechanisms ensure confidentiality and integrity of all stored and transmitted information.

7. Security Controls (Confidentiality, Integrity, Availability)

We apply rigorous safeguards including:

- Authentication: account-based access, password protection
- Authorization: role-based privileges, Access Authorization,
- Accounting: detailed activity logging and monitoring
- Operational controls: MLOps and AI development occur in controlled, segregated environments
- Marga AI security Authentications and Authorization support Google SSO as well as Apple SSO

7a. Data Segregation & Tenant Isolation

The Platform maintains logical separation between customer environments to prevent cross-tenant data access.

AI development, MLOps processes, and production systems operate in controlled and segregated environments with restricted access controls.

These measures ensure that customer data remains isolated and accessible only to authorized users within the relevant organization.

8. Data Accessed by the AI Coach

The AI Coach accesses only the data required for service delivery (account details, queries, usage



metadata).

Masters or administrators cannot access sensitive user information unless explicitly authorized.

8a. Use of Third-Party AI Sub-Processors

The Platform relies on certain third-party providers including but not limited to AI Model providers, Computation Hosting providers and other software and service and to deliver its core functionality.

Under applicable data processing agreements:

- Conversation data transmitted to such providers is retained for a limited period (not exceeding 30 days) for safety and abuse monitoring purposes.
- Such providers do not use customer data for model training.
- Retention by these providers is governed by their own data processing terms.
- In the event of a data erasure request, Marga AI will delete its own records within the 30-day period described above. Data already transmitted to AI infrastructure sub-processors may remain within their systems for up to 30 days from the date of transmission, in accordance with their contractual terms.

9. End User Agreement (EULA)

The Terms of Use act as the platform's EULA.

Both the Terms of Use and Privacy Policy outline how data is handled and must be accepted by every user.

10. Usage Reporting

The system produces comprehensive audit logs to support usage reporting, security monitoring, and regulatory compliance.

11. Account Termination and Offboarding

Upon termination of the Customer agreement or closure of an End User account:

- Platform access is disabled.
- Personal data is scheduled for deletion within 30 days.
- Any data required to be retained under applicable law will be isolated and retained solely for compliance purposes.
- Written confirmation of deletion can be provided upon request.

