

Data Privacy Policy for Client-Facing AI Tools (Azure Tenancy)

Effective Date: November 2025

Purpose and Principles

This policy outlines how Leading AI Ltd (“we”, “us”, “our”) collects, processes, retains, and protects data handled by our AI Assistant services (“the Service”), built using Azure OpenAI services and deployed within the client’s Azure tenancy. It aims to ensure compliance with the Data Protection Act 2018 and other applicable data protection legislation including but not limited to the General Data Protection Regulation (GDPR), as well as alignment with industry best practice and ISO 27001/42001 standards.

Leading AI adheres to the seven key principles of GDPR:

- Lawfulness, Fairness, and Transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

Leading AI Ltd is certified to ISO27001/242001 standards (certificate number 477642025).

Scope

This policy applies to all AI tools and services created by Leading AI that are provided to clients and operated within their dedicated Azure environments, specifically within the UK South Azure region.

Information We Collect

Prompts and Responses: We retain the prompts users enter into the AI Assistant and the responses generated by the Service.

User Identification: Each prompt and response is linked to a Microsoft Entra ID. This identifier allows the client to associate activity with individual users within their organisation. Leading AI Ltd does not have the capability to link the Entra ID back to a specific user identity and all prompt and response data is therefore anonymous to us unless it includes Personally Identifiable Information.

Sharing with Clients: We share prompts, responses, and associated Entra IDs only with the client for whom the AI Assistant is deployed.

Service Improvement: Retained prompts and responses are used solely to refine and improve our AI tools.

Handling of Personal Data

Inclusion of Personal Data in Prompts: Users are advised when they log in to the Service not to enter any unnecessary Personally Identifiable Information into their prompts. If users do enter such information into a prompt, it will be recorded as part of the prompt and may therefore be identifiable. However privacy is maintained as we do not share the data with anyone other than the client to whom the Service is provided.



Data Retention: Prompts, responses, and associated Entra IDs are retained by us for one year unless otherwise specified in the client contract.

Data Hosting and Processing: All data is hosted and processed exclusively within the UK South Azure region, inside the client's Azure tenancy. No client data held or processed by Leading AI Ltd is shared with third parties or processed outside of the UK.

Data Security

Built within Client's Azure Tenant: Our AI Assistants operate within the client's Azure environment, leveraging the client's existing data security measures, including compliance with their security policies and protocols.

Technical and Organisational Measures: We implement appropriate measures to protect retained data, including:

- Encryption of data at rest and in transit
- Logical access controls (e.g. user credentials, multi-factor authentication)
- Unique identification of users and administrators
- Regular security assessments and reviews
- Adherence to least privilege and need-to-know principles for access rights

Protection of Records: Records are safeguarded against loss, destruction, falsification, unauthorised access, and release.

Roles and Responsibilities

Client Responsibilities: The client is responsible for managing user access, defining authorised users, and setting data retention and deletion policies within their Azure tenancy.

Leading AI Ltd Responsibilities: We provide technical documentation, support, and guidance to ensure responsible operation of AI tools and compliance with data privacy requirements.

Reporting Incidents: All parties must report suspected data breaches or incidents immediately, in accordance with legislation and their own agreed procedures.

DPO: Leading AI's Data Protection Officer (to whom any suspected data breach should be reported) is Neil Watkins (neil.watkins@leadingai.co.uk).

Legal Compliance

Lawful Processing: All personal data is processed by Leading AI Ltd on the basis of legitimate interests and/or contract performance, as set out in Article 6 of GDPR in accordance with the Data Protection Act 2018 and other relevant legislation.

Contractual and Regulatory Requirements: Data handling, retention, and sharing comply with all contractual obligations and statutory requirements.

Changes to This Privacy Policy

We may update this Privacy Policy from time to time. Changes will be communicated by posting the revised policy on our website.

Contact Us

If you have any questions about this Privacy Policy, please contact:

Leading AI Ltd
124 City Road
London, EC1V 2NX
Email: info@leadingai.co.uk