Privacy & Security

Architecture Overview

Document Type:	Technical Overview
Classification:	Public — Prospective Users & Evaluators
Version:	1.0
Issued:	April 30, 2026
Issuer:	PurposeMapped

1. Purpose

This document provides a technical overview of the privacy and security architecture of the PurposeMapped platform. It is intended for prospective users, enterprise evaluators, and compliance reviewers seeking to understand how user data is handled, stored, and protected.

2. Data Privacy Principles

PurposeMapped is built on the premise that personal data belongs to the individual — unconditionally. The following principles govern all data handling on the platform.

2.1 No Training Use

User conversations and personal data are never used to train AI models — neither the user's own companion model nor any other model operated by PurposeMapped or third parties.

2.2 No Data Sharing

User data is never sold, shared, or transferred to third parties for any purpose, including advertising, research, analytics, or product development.

2.3 No Central Aggregation

Conversations are not aggregated, indexed, or analyzed at the platform level. No cross-user data processing occurs.

2.4 Single Instance Residency

All user data — conversations, memory, files, and configuration — resides exclusively within the user's dedicated instance. No data replication occurs outside that instance.

3. Infrastructure Architecture

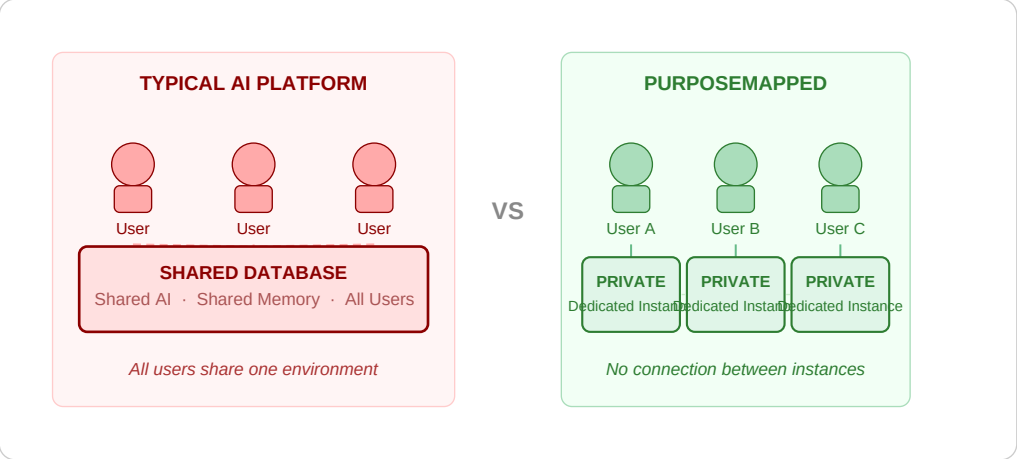
3.1 Dedicated Instance Model

Each PurposeMapped user is provisioned with a dedicated cloud instance hosted on Amazon Web Services (AWS) infrastructure. This instance is exclusive to the user and contains:

- The user's AI companion model and all associated configuration
- Complete conversation history and persistent memory
- User-specific files and uploaded content
- Isolated compute and storage resources

3.2 Architecture Diagram

The following diagram illustrates the structural difference between a typical shared-infrastructure AI platform and the PurposeMapped dedicated instance model.



3.3 Isolation Guarantee

Instances are isolated at the infrastructure level. There is no shared database, no shared compute, and no shared memory between users. One user's instance has no network path to another user's instance.

3.4 Comparison to Familiar Services

PurposeMapped's dedicated instance model is comparable to the private storage isolation model used by services such as Dropbox — where each user's data occupies a private, inaccessible bucket — except applied to the full AI stack, not just file storage. Each user receives their own private server, AI model, memory, and compute environment.

4. Access Control

4.1 Authorized Access Only

Instance access is restricted — available only through an authorized service request process. Routine access to user instances by PurposeMapped personnel does not occur and is not permitted outside of formal, documented service procedures.

4.2 User Data Isolation

Each AI companion is trained exclusively on interactions with its assigned user. The companion is never influenced by, exposed to, or contaminated by data from other users.

4.3 Independent Instance Operation

Each instance operates independently of all others. Other users' activity — including load, data changes, or configuration updates — has no effect on a given user's instance.

5. Summary

The following table summarizes the key privacy and security commitments of the PurposeMapped platform.

Principle	PurposeMapped Commitment
AI Training	User data is never used to train any AI model
Data Sharing	Data is never sold, shared, or transferred to third parties
Infrastructure	Dedicated per-user AWS instance — fully isolated
Instance Access	Restricted — authorized service request only
Cross-User Influence	None — instances are fully isolated from one another
Data Residency	Exclusive to the user's own instance

For questions regarding this document, contact support@purposemapped.com