EPIC TEST QUEST

Security & Privacy

A clear, transparent breakdown of how Wizzo accesses, processes, stores, and protects your data.

Version: February 2, 2025

Classification: Confidential

Prepared for: Customer Security & Legal Review

CONFIDENTIAL — FOR AUTHORIZED RECIPIENTS ONLY

Table of Contents

Overview

Wizzo is an AI-powered Slack app that helps teams generate test cases from requirements. This document provides a comprehensive view of our security and privacy practices, including what data we access, how we process it, and the measures we take to protect it.

This document is intended for review by customer security and legal teams during vendor assessment, procurement, or compliance processes.

At a Glance: Wizzo & Your Data

Area	Summary
Data access	Only what you explicitly share in Wizzo interactions.
Data storage	Minimal, purpose-limited, encrypted at rest and in transit.
AI processing	Google Gemini API; data not retained or used for training.
Hosting region	European Union (Frankfurt, Germany).
AI processing region	United States (protected by SCCs).
Integrations	Optional Jira and GitHub connections; OAuth-based.
Retention	User-controlled deletion; automatic cleanup of temporary data.

Data Access in Slack

Wizzo only accesses data that users explicitly provide through interactions with the app:

- Messages sent directly to Wizzo in the app's DM channel or Home tab
- Content shared in Quality Party threads where Wizzo is explicitly invoked
- Files attached to messages directed at Wizzo (images, PDFs for visual test generation)

What Wizzo Does NOT Access

- Private channels where Wizzo is not invited
- Direct messages between users
- Message history or archives
- User presence or status information
- Email addresses or phone numbers beyond what Slack provides in the user profile

Data We Store

Wizzo stores the following data to provide its core functionality:

Data Type	Purpose	Retention
Products & Features	Organize test cases	Until user deletes
Test cases	Core functionality	Until user deletes
Session context	Maintain conversation flow	72 hours (auto-deleted)
Draft test cases	Review before saving	24 hours (auto-deleted)
Quality Party sessions	Collaborative discussions	Configurable (24–96 hours)
Integration tokens	Jira/GitHub access	Until user disconnects
User preferences	Personalization	Until user deletes account

Data We Never Store

- Raw Slack message content beyond active sessions
- Passwords or authentication credentials (OAuth tokens only)
- Credit card or payment information (handled by Slack)
- Personal health information
- Biometric data

AI Model Processing

Wizzo uses **Google Gemini** for AI-powered test case generation.

Aspect	Detail
AI Provider	Google (Gemini API)
Processing Location	United States
Data Retention by AI	None — data is not retained after processing
Training Data	Not used — your data is never used to train AI models
Transfer Protection	Standard Contractual Clauses (SCCs) approved by the European Commission

What Gets Sent to the AI

- Requirements text you provide
- Product/feature context you've defined
- Attached images or PDFs (for visual test generation)
- Selected personas and focus areas

What Does NOT Get Sent

- Your Slack user ID or personal information
- Your workspace name or team information
- Historical test cases or products
- Integration credentials or tokens

Processing occurs within Google Cloud's infrastructure in the United States. Data transfers to the US are protected by Standard Contractual Clauses (SCCs) approved by the European Commission.

AI Limitations & Human Oversight

Important: AI-generated content has inherent limitations:

- **Accuracy** — AI outputs may contain errors, inaccuracies, or omissions.
- **Context** — AI may misinterpret requirements or generate test cases that don't match your intent.
- **Completeness** — AI may not cover all edge cases or testing scenarios.

Human oversight is required:

- Always review AI-generated test cases before use.
- Validate that outputs meet your quality standards.
- Do not rely on AI outputs for safety-critical, medical, legal, or financial decisions without independent verification.
- You are responsible for any decisions made based on AI-generated content.

Integrations (Jira & GitHub)

Jira Integration

Aspect	Detail
Authentication	OAuth 2.0 (user-level)
Scope	Read issues, write comments
Data flow	Issue data fetched on-demand, not stored permanently
Token storage	Encrypted, per-user

GitHub Integration

Aspect	Detail
Authentication	GitHub App (workspace-level)

Aspect	Detail
Scope	Read PRs and issues, write comments
Data flow	PR/issue data fetched on-demand, not stored permanently
Installation	Managed by workspace admins

Both integrations are optional and can be disconnected at any time.

Data Encryption & Infrastructure

Encryption

Layer	Standard
In transit	TLS 1.2+ for all connections
At rest	AES-256 encryption for stored data

Infrastructure

- **Application hosting:** Secure cloud infrastructure
- **Database:** Supabase (PostgreSQL with Row Level Security)
- **Hosting region:** European Union (Frankfurt, Germany — AWS eu-central-1). No data is replicated outside the EU except for AI processing as described above.
- **Backups:** Automated daily backups stored in the same EU region (eu-central-1). Encrypted at rest using AES-256.

Security Features

- Row Level Security (RLS) enforced on all database tables
- Service role separation for application vs. admin access
- Automatic security advisories via Supabase

Data Residency

Wizzo operates from a single hosting region: European Union (Frankfurt, Germany — AWS eu-central-1).

Data Category	Location	Notes
Application data	EU (Frankfurt)	Primary database
Backups	EU (Frankfurt)	Same region as primary
AI processing	United States	Protected by SCCs; no data retained

Wizzo does not currently offer custom regional data residency. All customer data is hosted in the EU region described above. If your organization has specific data residency requirements, please contact us at legal@epictestquest.com.

Data Retention & Deletion

Automatic Cleanup

Data Type	Retention Period
Conversation sessions	72 hours of inactivity
Draft test cases	24 hours after creation
Quality Party sessions	Based on configured duration (24–96 hours)
Expired OAuth tokens	Immediate on expiration

User-Initiated Deletion

- Delete individual test cases, products, or features via the Home tab
- Disconnect integrations to remove stored tokens
- Contact support to request full data deletion

Workspace Removal

When Wizzo is uninstalled from a workspace, all associated data is queued for deletion within 30 days.

Access Control & Internal Security

Application Access

- Multi-workspace isolation via team_id enforcement
- No cross-workspace data access
- Bot tokens scoped per workspace

Internal Practices

- Principle of least privilege for all systems
- Regular security reviews of dependencies
- No production data access without audit logging

Admin Controls & Auditability

Workspace Admins Can

- Install/uninstall Wizzo for the workspace
- Manage GitHub App installation (workspace-level)
- View which users have connected Jira (via Jira admin console)

Audit Capabilities

- Session activity logged with timestamps
- AI call counts tracked per session
- Integration connection/disconnection events recorded

Threat Protection & Safe Use

Input Validation

- All user inputs sanitized before processing
- File uploads validated for type and size
- Rate limiting on AI calls (20 per session, 5 per minute)

Prompt Injection Protection

- System prompts isolated from user content
- Output validation before display
- Intent detection filters for malicious patterns

Recommended Practices

- Do not share sensitive credentials in messages to Wizzo
- Review generated test cases before sharing externally
- Use Wizzo in appropriate channels (not for confidential discussions)

In-Product Feedback & Support Data

Feedback Collection

- Thumbs up/down on generated test cases (optional)
- Feedback stored with session context for quality improvement

- No personal data included in feedback analysis

Support Requests

- Handled through Slack or designated support channels
- Support data retained only as long as needed to resolve issues

Compliance & Legal

Framework Alignment

Framework	Status
GDPR	Compliant (EU data hosting, user rights supported)
SOC 2	Via sub-processors (Supabase, Google)
Data Processing	DPA available on request

Sub-processors

Wizzo uses cloud infrastructure and AI model providers as sub-processors.

Sub-processor	Purpose	Location	Certifications
Google (Gemini API)	AI processing	United States	SOC 2, ISO 27001
Supabase	Database & auth	EU (Germany)	SOC 2 Type II
Slack	Platform integration	United States	SOC 2, ISO 27001
Atlassian (Jira)	Optional integration	US or EU	SOC 2, ISO 27001
GitHub	Optional integration	United States	SOC 2, ISO 27001

Legal Basis for Processing

- **Contract performance:** Providing the Wizzo service you requested
- **Legitimate interest:** Service improvement, security
- **Consent:** Optional features like feedback collection

Contact

For inquiries related to security, privacy, or data protection:

Purpose	Contact
Data Protection / Privacy	legal@epictestquest.com
Security / Vulnerability Reports	security@epictestquest.com
General Legal	legal@epictestquest.com

Response time: Within 48 hours for security and data protection matters.

Updates

This page is reviewed quarterly and updated as our practices evolve. Material changes will be communicated via the Wizzo Home tab or workspace notifications.

Changelog

Date	Change
February 2, 2025	Added Data Residency section, backup location info, explicit Data Protection contact.
January 21, 2025	Added explicit hosting region, AI processing location, and sub-processor list.
January 2025	Initial publication of Security & Privacy overview.