ALMO SECURITY & COMPLIANCE POLICY

Version: 1.0

Date: March 2026

Document Owner:

Nikkhil Gupta

Director: VI8 Ltd

71-75 Shelton Street

Covent Garden

London

WCH2H 9JQ

1. EXECUTIVE SUMMARY

Almo is a Microsoft Outlook add-in published on Microsoft AppSource and operated as a cloud-hosted Software-as-a-Service (SaaS) solution on Microsoft Azure in the Central US region. This document describes the technical and organizational measures used to protect customer data and support customer security and compliance assessments for deployments such as Tel Aviv Municipality.

2. PUBLISHER AND ORGANIZATION DETAILS

Provider / Legal Entity: VI8 Ltd

Registered Office: 71-75 Shelton Street, Covent Garden, London - WC2H 9JQ, United Kingdom

Company Registration Number: 10036231, United Kingdom

Website: https://getlamo.com

Microsoft AppSource Listing:
https://marketplace.microsoft.com/en-us/product/WA200010090?tab=Overview

Support Contact: support@vi8.raiseaticket.com

Security Contact:nikkhilgupta@vi8.co.uk

Legal Contact: nikkhilgupta@vi8.co.uk

3. MICROSOFT APPSOURCE AND MICROSOFT 365 PROGRAMS

Almo is listed on Microsoft AppSource as an Outlook add-in. As part of the listing process, the application and publisher are reviewed against Microsoft's requirements for security, data handling, and publisher verification applicable to Microsoft 365 apps.

Relevant Microsoft documentation :

- Microsoft 365 App Compliance Program overview:

  https://learn.microsoft.com/en-us/microsoft-365-app-certification/overview

- Web app security and compliance information:

  https://learn.microsoft.com/en-us/microsoft-365-app-certification/web/web-apps

While this Microsoft validation is not a substitute for your own risk assessment, but it provides independent assurance that the app and publisher meet Microsoft's baseline security and compliance requirements.

4. HOSTING, INFRASTRUCTURE AND RESPONSIBILITIES

Hosting Platform: Microsoft Azure (public cloud)

Primary Region: Central US (Azure region)

Service Model: Platform as a Service (PaaS) / Web App

Almo runs as an Azure web application and uses Azure managed services for data storage. Microsoft is responsible for the security of the underlying cloud infrastructure. Almo's publisher is responsible for the security of the application, configuration, and operational processes.

Key Azure documentation (for reference):

- Azure encryption overview (encryption at rest and in transit):

https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview

5. DATA ENCRYPTION AND PROTECTION

5.1 Encryption in Transit

- All connections between client, Outlook add-in, Almo web application, and backend services use HTTPS with TLS (TLS 1.2 or higher).

- TLS certificates are managed via Azure; certificates are renewed automatically.

- Non-encrypted protocols are not exposed for customer traffic.

5.2 Encryption at Rest

- All customer data stored in Azure managed storage/database services is encrypted at rest using Azure's built-in encryption.

- Backup data is also encrypted at rest using the same encryption mechanisms as primary storage.

- Encryption keys are managed by Azure by default. If a customer requires customer-managed keys (CMK), this can be evaluated separately.

5.3 Communication with Azure DevOps Services

- Almo web app communicates with Azure DevOps Services directly using Microsoft provided client SDK.
- No data in this flow passes through any VI8 managed APIs or end points. All communication is direct.

5.3 Secrets Management

- Administrative and application secrets (for example, service principals, connection strings) are stored in secure configuration mechanisms such as Azure Key Vault or equivalent secret storage.

- Access to secrets is restricted to a minimal set of administrative identities.

6. AUTHENTICATION, AUTHORIZATION AND ACCESS CONTROL

6.1 End-User Authentication

- End-user authentication is performed using Microsoft's identity platform (Microsoft Entra ID / Azure AD) via OAuth 2.0 and OpenID Connect.

- The add-in relies on the customer's existing Microsoft 365 tenant security controls, including conditional access and multi-factor authentication (MFA) for end users where configured by the customer.

6.2 Administrative Access

- Administrative access to the production environment is restricted to a very small, named set of administrators (1).

- Multi-factor authentication (MFA) is enforced for all accounts.

- Access follows the principle of least privilege; administrators receive only the minimal access required to perform their role.

- Administrative access is logged (for example, via Azure activity logs and application logs).

6. ENVIRONMENT SEPARATION

Almo uses separate environments for:

- Development

- Test / Staging

- Production

Each environment has:

- Separate resources (web apps, databases, storage accounts)

- Separate credentials and configuration

- Restricted access appropriate to its purpose

Production data is not used in development or test environments.

8. LOGGING, MONITORING AND AUDIT

- Relevant operations-related events (for example, authentication events, administrative actions, key application errors) are logged.

- Logs are retained for a period sufficient for security investigations and troubleshooting (for example, at least 90 days; configurable over time).

- Access to logs is restricted to authorized personnel.

- Azure-native monitoring and alerting are used to detect anomalous behaviour and significant failures.

9. DATA CATEGORIES, HANDLING AND RETENTION

9.1 Data Collected and Processed

Depending on configuration and use, Almo typically processes:

- Task-related metadata such as task title, description, due date, status, and priority.

- User preferences and configuration settings.

- Minimal technical and telemetry data necessary for security, support and operation of the service.

Almo does not intentionally process or store:

- Email message bodies, subjects, sender, recipient details or any metadata.

- Attachments.

- Calendar data.

9.2 Data Location

- Customer data processed by Almo is stored in Microsoft Azure in the Central US region.

- Data is not intentionally transferred to systems outside Azure except where required for legal reasons or with explicit customer agreement.

9.3 Data Retention and Deletion

- Customer data is retained for as long as the customer’s account and subscription remain active and is used only to provide the Almo service.

- Upon account closure or written request, application data is deleted or anonymized within a defined period (for example, within 30 days), subject to technical constraints and legal requirements.

- Backups are retained per Azure's standard backup retention for the services in use; backup copies are not actively edited but expire and are deleted in line with that retention.

10. SUBPROCESSORS AND THIRD PARTIES

- Primary subprocessor: Microsoft Corporation, providing Azure infrastructure and platform services (compute, storage, database, networking, identity).

- No customer data is shared with unrelated third parties for analytics, marketing, or advertising purposes.

- If additional subprocessors are introduced in the future, they will be documented and communicated to affected customers as required.

11. INCIDENT RESPONSE AND NOTIFICATION

11.1 Detection

- Security-relevant events are monitored using Azure-native tools and application logging.

- Indicators of compromise or abnormal activity are investigated without undue delay.

11.2 Response

In the event of a suspected or confirmed security incident affecting customer data, the response process includes:

1. Initial triage and containment.

2. Investigation and root cause analysis.

3. Remediation and implementation of corrective measures.

4. Documentation of the incident and lessons learned.

11.3 Notification

- If a personal data breach or security incident with material impact on customer data is confirmed, affected customers will be notified without undue delay and within applicable legal timeframes (for example, within 72 hours where GDPR applies).

- Notifications will include known details about the incident, data impacted (if known), and remediation steps taken or planned.

12. SECURITY PRACTICES AND VULNERABILITY MANAGEMENT

- Changes to the application are reviewed before deployment.

- Dependencies are periodically reviewed and updated; critical and high-risk security updates are prioritized.

- Secrets and keys are stored using secure mechanisms and rotated periodically.

- Known security vulnerabilities are assessed and remediated according to severity.

13. SUMMARY OF KEY SECURITY COMMITMENTS

VI8 attests that for the Almo service:

- Almo operates as a SaaS service on Microsoft Azure in the Central US region.

- Data is encrypted in transit (TLS) and at rest (Azure-managed encryption).

- MFA is enforced for all accounts.

- Development, test and production environments are separated.

- Production access is limited to a small set of named administrators and is based on least privilege.

- Administrative access and key security events are logged.

- Customer data is not sold and is not shared with unrelated third parties, including for marketing.

- The company is prepared to cooperate with the municipality's security and compliance review processes.

15. CONTACT

Support Contact: support@vi8.raiseaticket.com

Security Contact:nikkhilgupta@vi8.co.uk

Legal Contact: nikkhilgupta@vi8.co.uk

Document Classification: Customer-Shareable