

SECURITY OVERVIEW

Eva in Microsoft Teams

What Eva accesses, how it is used, and what your IT team controls.

Prepared for customer IT and security review · September 2026 · Version 1.0

Latest version online: evergrowth.com/company/security-trust/microsoft-teams



SOC 2 Type 2

Audited



ISO 27001:2022

Certified



GDPR

Article 28 processor



No training

on customer data

At a glance

What it is	An additional chat surface for Eva, the AI assistant your team already uses in the Evergrowth web application. It introduces no new data store, no new user directory and no new permission model.
Microsoft 365 permissions requested	<code>identity</code> only, which provides the name and email address of the person talking to Eva. No Microsoft Graph permissions and no tenant-wide admin consent.
What Eva can read in Teams	Only the messages sent to her in a user's own 1:1 chat with her. No mailbox, calendar, files, SharePoint, OneDrive, directory, or any other channel or chat.
Who can use it	Only people who already hold an Evergrowth account in the linked workspace. Membership of your Teams tenant grants nothing on its own; there is no auto-provisioning.
What Eva can do	Exactly what that individual can already do in the Evergrowth web application, enforced by a per-user token derived from their own role and permissions.
Data it touches	Your own Evergrowth workspace data, plus public web research. Eva holds no credentials for your CRM, your Microsoft 365 tenant or any other system of yours.
Inbound request security	Every message carries a Microsoft-signed RS256 token, validated against Microsoft's published keys with issuer, audience and service URL all pinned, then de-duplicated by message ID.
Model providers	Enterprise endpoints only, all under contractual terms that prohibit training on your data. Default agent routing is AWS Bedrock in <code>eu-west-1</code> (Ireland).
Data residency	Default model routing runs in the EU. Any transfer outside the EEA and UK is made under Standard Contractual Clauses. EU-only processing is available on request as a written amendment to the DPA.

Eva in Microsoft Teams: Security Overview · v1.0 · September 2026

1 / 9

Retention on exit	Data is returned or deleted at your choice. Absent a request, all personal data is permanently deleted within 30 calendar days of termination.
How to remove it	A Teams administrator removes the app and the workspace link is retired. Nothing remains consented in Microsoft Entra, because nothing was consented.

This page covers the Teams surface specifically. Evergrowth’s platform-wide security posture, data flow and legal terms are published in full and are the authoritative source for everything beyond Teams:

Security & Trust: evergrowth.com/company/security-trust

Data Flow Overview: evergrowth.com/company/data-flow

Data Processing Agreement: evergrowth.com/legal/dpa/v1-0

01

What Eva in Teams is

Eva is Evergrowth’s AI assistant for revenue teams. The Microsoft Teams app is an additional client for the same Eva your users already have at app.evergrowth.com. It is a different way to reach a system the user is already entitled to use, which means your existing Evergrowth access review continues to govern it.

It is delivered as a standard Microsoft Teams bot on Azure Bot Service. Today it operates in **1:1 personal chat only**; the app package declares the [personal](#) scope and nothing else, so Eva cannot be added to a team channel or a group chat. Channel support will arrive with the Microsoft Teams Store listing as a new, separately reviewable version of the app.

What the app can access inside Microsoft 365

The app package requests exactly one Teams permission: `identity`.



Eva can see

- The messages a user sends her in that user's own 1:1 chat with her.
- The name and email address of the person talking to her, read from the conversation roster, solely to match them to their Evergrowth account.



Eva cannot see or do

- No mailbox, calendar, OneDrive, SharePoint or Teams file access.
- **No Microsoft Graph application permissions**, so no tenant-wide admin consent is requested and Evergrowth holds no standing directory or content permission in your tenant.
- No access to any other channel, chat or conversation. Single sign-on and the resource-specific read permissions that would allow reading a wider thread are **not present** in the deployed package.
- No ability to message your people proactively, and no ability to enumerate your directory.

Nothing is written into or retained inside Microsoft Teams beyond the messages of the conversation itself.

How a person is authorised

Authorisation is anchored to your existing Evergrowth entitlements, in three steps.

1

Tenant binding. A Microsoft 365 tenant is bound to exactly one Evergrowth workspace. The binding is established on first use by a person who is already a member of that workspace, and is retired automatically when the app is removed from the tenant.

2

User matching, on every message. The sender's Microsoft 365 email address is resolved to an existing Evergrowth user *within that bound workspace*. Where no matching Evergrowth account exists, Eva does not answer; she replies that the person must be added by an Evergrowth administrator. Matching never crosses workspaces and is refused outright where it would be ambiguous.

3

Least privilege. Eva then operates under a per-user access token whose capabilities are derived from that individual's own role and permissions in Evergrowth. **Eva in Teams can see and do exactly what that person can see and do when logged into the Evergrowth web application, and nothing more.** Revoking or downgrading an Evergrowth account immediately changes what Eva will do for that person in Teams.

This matters for your review: Eva in Teams adds no new access path to your data. It inherits the one you have already approved.

04

What Eva accesses on the Evergrowth side

All of it is your own Evergrowth workspace data, subject to the per-user permissions above. Each customer workspace is logically isolated; every record carries a company identifier and access is validated against the requesting organisation before any record is returned.

Reads	Accounts and contacts, ICP verticals and ecosystems, personas and buying committees, plays, saved views and filters, agent configuration, account plans, workflow and task status, and CRM fields already synced into Evergrowth.
Writes, only where the individual's own role permits	Create, update and delete verticals, personas, plays, agents, saved views and account plans; tag accounts and contacts; import accounts and contacts; start exports; trigger and schedule Evergrowth workflows.
External research	When asked to research a company or a person, Eva performs public web search and page retrieval. These are outbound requests to the public internet. Eva does not reach back into your systems, your network or your Microsoft 365 tenant to do this.
Tooling limits	Agents operate with a hand-picked tool set, namely web search, scraping and internal lookup. There is no code execution, no filesystem access, no shell and no arbitrary network access. Writes to customer systems travel through separate authenticated paths.

05

Personal data processed

The platform neither requests nor requires payroll, employee, health or payment card data at any point. Personal data processing is limited to business contact and professional profile data for people matching the ICP and buyer personas you approve.

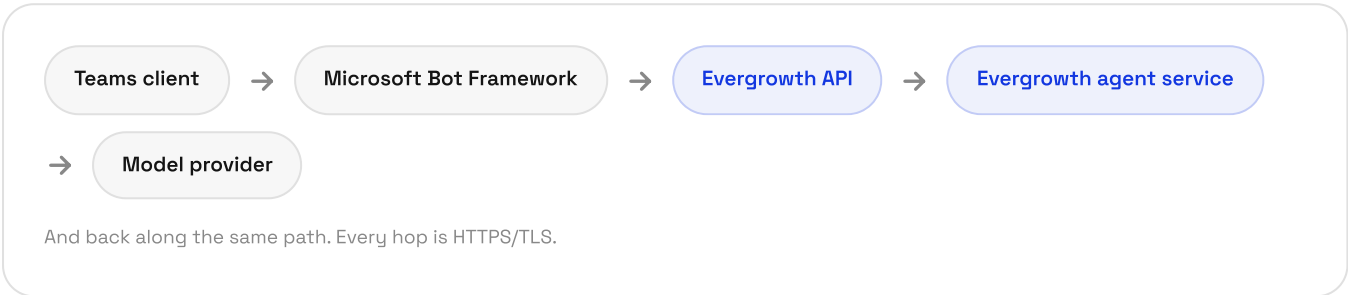
CATEGORY	FIELDS
Contact identifiers	Full name, job title, email address, phone number, LinkedIn profile
Professional profile	Employment history, education, skills, languages, profile summary, location, profile photograph, follower and connection counts
Qualification record	The persona and profile match result, with the reasoning behind it

What actually reaches a model is narrower still: the personal data in a prompt is limited to what the qualification decision requires, being name, job title, LinkedIn profile and employer. No profile photograph, no employment history and no special category data is sent to a model.

Two qualification gates run inside the workspace before any external source is called: the company must match the profile you approved, and the person must match a persona you defined. Minimisation is therefore applied at the point of collection rather than afterwards, under Article 5(1)(c), and the reason each contact qualified is recorded at that moment.

06

Data flow and transport security



Every inbound request from Microsoft is cryptographically authenticated before it is processed:

- An RS256 JSON Web Token issued by the Bot Framework service, validated against Microsoft’s published signing keys.
- Issuer pinned to `https://api.botframework.com`, and audience pinned to Evergrowth’s own bot application ID, so a token minted for a different bot is rejected.
- The token’s `serviceurl` claim must match the service URL on the activity itself, so a captured token cannot be replayed against a different connector.
- Activities are de-duplicated by message ID, so a replayed message is not processed twice.

More broadly, every request into the platform enters through a signed JWT or a service API key carrying the requesting user’s organisation identifier, which scopes all downstream access. Users authenticate through a dedicated identity provider, with two-factor authentication available by authenticator app or emailed code.

07

AI processing and model providers

Eva’s inference is served exclusively by enterprise model endpoints, all operating under contractual terms that prohibit training on your data. There are no consumer endpoints and no providers in non-aligned jurisdictions.

PROVIDER	TRAINING	RETENTION
AWS Bedrock	Inputs and outputs are not used to train Amazon or third-party models	Prompts and completions are not stored or logged. Default routing for Evergrowth agents, in <code>eu-west-1</code> .
Microsoft Azure OpenAI	Prompts and completions are not used to train models	Retained up to 30 days for abuse monitoring. Modified abuse monitoring, which removes storage, is available on approved application.

PROVIDER	TRAINING	RETENTION
OpenAI	API inputs and outputs are not used for training	Retained for abuse monitoring. Zero data retention available to eligible API customers.
Google Gemini API	On paid services, prompts and responses are not used to improve Google products	Logs retained up to 55 days by default, configurable to 7, 14 or 28. Zero data retention available on approved request.

Which endpoint serves a given request depends on the task. Where a customer requires processing pinned to EU regions, that is scoped jointly and recorded as a written amendment to the Data Processing Agreement (see section 8).

Safeguards against AI-specific risks

- ✓ **Prompt injection.** System prompts are authored, peer-reviewed, versioned and loaded server-side from a controlled registry. Third-party content, including web pages, CRM records and search results, enters the model strictly as data inside delimited user-message blocks, never concatenated into the system prompt. Outputs are bound to typed schemas, so an injected directive cannot reach a downstream system as free-form text. Maps to OWASP LLM01 and LLM05.
- ✓ **Excessive agency.** Narrow per-agent tool sets, no code execution, filesystem or shell. Maps to OWASP LLM06.
- ✓ **Workspace-scoped retrieval.** Vector retrieval and embeddings are scoped per workspace and never shared across tenants.
- ✓ **Traceability.** Every agent run produces a structured trace covering prompt version, tool calls, inputs, outputs, latency and token usage, captured in a monitored pipeline.
- ✓ **EU AI Act.** Evergrowth’s agents perform B2B research, qualification and copy generation, and do not make decisions in the Annex III high-risk domains. A human reviews any action affecting external parties.

08
Hosting, residency and retention

- ✓ **Infrastructure.** Workloads run on AWS with KMS-encrypted secrets and cluster-level audit logging. Persistent stores use managed PostgreSQL with KMS encryption at rest and Multi-AZ availability for primary databases. Data is encrypted in transit and at rest.
- ✓ **Model routing.** Default agent inference runs on AWS Bedrock in `eu-west-1`, Ireland, which does not store prompts or completions.
- ✓ **Transfers.** Some processing takes place outside the EEA and the UK where necessary to provide the service. Any such transfer is made under Standard Contractual Clauses or other appropriate safeguards under Chapter V of Regulation (EU) 2016/679, and sub-processors outside the EEA and UK are required to provide equivalent safeguards (DPA clauses 5.1 and 5.2).

- ✓ **EU-only on request.** Processing can be pinned to EU regions for customers with a data residency requirement. Scope, timeline and any commercial impact are agreed in writing and recorded as an amendment to the Data Processing Agreement before the commitment is made. A US-only equivalent exists through the same mechanism.
- ✓ **Retention and deletion.** On expiry of the agreement personal data is returned or deleted at your choice, and sub-processors are required to do the same. Absent a written request, all personal data is permanently deleted within 30 calendar days of termination (DPA clauses 9.1 and 9.2).
- ✓ **In-product deletion.** A user can delete an Eva conversation thread, which removes the thread and its stored agent state.

69

Sub-processors

Four categories of sub-processor receive data, and each receives only what its function needs.

CATEGORY	WHAT LEAVES THE WORKSPACE, AND WHY
Data providers	A company name, job title and country, to identify people holding that role. For a contact you already hold, the identifier for that person, to retrieve business contact information.
Verification	A single email address or phone number, to confirm it is valid and deliverable before use. Runs only where you enable verification.
Model providers	Prompt contents, which include account and contact context, for inference.
Platform services	Hosting, monitoring of processing including AI processing, support and billing, together with product and session analytics in the user’s browser.

Each sub-processor is named, with its country of processing, in the **sub-processor register**, which Evergrowth provides on request and during a security review. Under DPA clause 4.2 the register is maintained and you are notified of material changes, with a right to object on reasoned grounds within seven calendar days. Evergrowth remains fully responsible for its sub-processors under clause 4.4.

10

Certifications and compliance

SOC 2 Type 2	Independently audited over an observation period, with no exceptions identified. Report available during a security review.
ISO 27001:2022	Certified. Certificate available during a security review.

GDPR	Regulation (EU) 2016/679. You are the controller; Evergrowth is the processor under Article 28, acting on your documented instructions through a formal DPA. Lawful basis for contact processing is legitimate interest under Article 6(1)(f), recorded per individual rather than asserted as policy.
UK, US, Canada	UK GDPR; CCPA/CPRA, VCDPA, CPA, CTDPA and UCPA, under which Evergrowth acts as service provider or processor and data is never sold or shared; PIPEDA and Quebec Law 25.
Data subject rights	Individuals retain rights under Articles 15 to 21 including the right to object under Article 21. Requests reach you as controller, and the DPA commits Evergrowth to assist. Because each contact carries the reason it qualified and the source it came from, the answer already exists on the record.

11

Controls your IT team retains

- ✓ **Installation is admin-gated.** The app package is uploaded by a Microsoft 365 or Teams administrator through the Teams admin center.
- ✓ **Scope it to named users.** Standard Teams app permission and setup policies apply, so the app can be limited to a pilot group rather than the whole tenant.
- ✓ **Removal is immediate and complete.** Removing the app from the tenant retires the workspace binding.
- ✓ **Nothing to revoke in Entra.** Because no Microsoft Graph application permissions and no tenant-wide consent are requested, Evergrowth holds no standing Microsoft 365 data permission.
- ✓ **Evergrowth entitlements remain the control plane.** Only people who already hold an Evergrowth account can use Eva in Teams, and only within their own permissions.
- ✓ **Audit trail.** Access and processing activities are logged and monitored, and every agent run is individually traceable.

12

Technical appendix

Inbound endpoint	<code>POST https://api.evergrowth.com/api/teams/messages</code> , TLS only
Inbound authentication	Bot Framework RS256 JWT; keys from <code>https://login.botframework.com/v1/.well-known/openidconfiguration</code> ; issuer, audience and <code>serviceurl</code> all validated; message-ID de-duplication
Teams manifest permissions	<code>identity</code>
Teams bot scopes	<code>personal</code> (1:1 chat only)

Microsoft Graph permissions	None
Tenant-wide admin consent	Not requested
Valid domains in manifest	app.evergrowth.com
Default model routing region	AWS Bedrock eu-west-1 , Ireland
Installation route	Evergrowth app → Integrations → "Add to Teams" downloads the app package; a Teams administrator uploads it in the Teams admin center
Publisher	Evergrowth, publisher domain evergrowth.com , verified in Microsoft Entra
Privacy policy	www.evergrowth.com/privacy-policy
Terms of use	www.evergrowth.com/terms

13

Available on request

- ✓ SOC 2 Type 2 report and ISO 27001:2022 certificate.
- ✓ Current sub-processor register, naming each sub-processor and its country of processing.
- ✓ Full OWASP LLM and EU AI Act control mapping, under NDA.
- ✓ A technical walkthrough of the architecture with your security team.
- ✓ Master Services Agreement and the Data Processing Agreement annexed to every customer contract.

Evergrowth is the processor and the customer is the controller for personal data in the workspace, under Article 28 of Regulation (EU) 2016/679. Where this summary and the executed agreements differ, the agreements prevail. Platform-wide detail is published at [evergrowth.com/company/security-trust](#), [evergrowth.com/company/data-flow](#) and [evergrowth.com/legal/dpa/v1-0](#). The latest version of this document is at [evergrowth.com/company/security-trust/microsoft-teams](#).