Privacy Policy

Version 1.0

Effective Date: October 13, 2025

Last Updated: January 11, 2026

Hypoth, Inc. ("Company", "we", "us", or "our") is committed to maintaining robust privacy protections for our users. Hypoth, Inc. is a Delaware corporation.

This Privacy Policy ("Policy") describes how we collect, use, and safeguard the personal information you provide when using Olllo – your personal AI career manager, accessible via https://olllo.ai, our mobile applications, and any other websites, subdomains, applications, or services operated by or on behalf of Hypoth, Inc. (collectively, the "Services").

By accessing or using our Services, you agree to the terms of this Privacy Policy and our Terms of Use. If you do not agree, please discontinue using the Services.

I. Information We Collect

We collect two types of information: **Personal Information** and **Non-Personal Information**.

1. Personal Information

We collect only the information necessary to provide and improve our Services, including:

- **Account Information**: Email address (required for account creation and authentication), optional name or display name
- **Profile Information**: Job title, department, company name, company size, industry, years in role, managerial role
- **Preferences**: Time zone, locale, theme preferences, AI interaction tone, notification settings
- **User-Generated Content**: Accomplishments, goals, reflections, notes, and related content you enter into the app

- **Communications**: Messages you send to us for support or feedback

All personal data is stored securely and associated with your account created through Clerk, our identity provider.

2. Information Collected Automatically

When you use Olllo, we may automatically collect:

- **Device Information**: Device and browser type, operating system, device identifiers
- **Usage Data**: How you interact with our Services, features you use, time spent, referring and exit pages
- **Log Data**: IP addresses, date and time of access, session and authentication state
- **Anonymous Metrics**: Performance and security metrics that do not identify individual users

We use cookies and similar technologies managed by Clerk to maintain sessions and authenticate users. Clerk may set persistent and session cookies to remember your login state.
We do not use tracking cookies for advertising or behavioral profiling.

3. Children's Privacy

Olllo is intended for users **13 years of age or older**.

We do not knowingly collect or solicit information from anyone under 13. If you believe a child under 13 has provided us personal information, please contact privacy@olllo.ai, and we will delete the information promptly.

II. How We Use Your Information

We use your Personal Information to:

- **Provide Services**: Operate, maintain, and improve the Services
- **Authentication**: Authenticate your account and maintain secure sessions
- **Personalization**: Customize your experience and provide AI-powered insights
- **Communications**: Send essential account-related communications (e.g., verification, security, policy updates) and respond to your inquiries
- **Security**: Detect and prevent fraud, abuse, and security threats
- **Analytics**: Understand usage patterns to enhance features and user experience
- **Legal Compliance**: Comply with legal obligations and enforce our terms

III. AI Processing and Your Data

1. How AI Uses Your Data

Our AI features process your User Content to:

- Generate personalized accomplishment summaries using the STAR (Situation, Task, Action, Result) framework
- Provide goal recommendations and track progress insights
- Facilitate structured reflection conversations
- Extract and organize professional achievements
- Detect and redact personally identifiable information (PII) for privacy protection

2. AI Data Handling Practices

- **Secure Processing**: AI processing occurs on secure servers with encrypted connections
- **No Model Training**: Your content is NOT used to train general AI models
- **Data Minimization**: We process only the data necessary for each AI feature
- **Storage**: AI-generated insights are stored with your account data and subject to the same protections
- **Human Oversight**: AI outputs are designed to assist, not replace, your professional judgment

3. AI Providers

We use Vercel AI Gateway to power our AI features. Vercel AI Gateway routes requests to various AI model providers to deliver AI-powered functionality. Your content is transmitted to these providers solely for processing your requests and is subject to their respective privacy policies and data processing agreements. The specific AI models used may change as we improve our Services.

IV. Information Sharing and Third-Party Services

We do not sell, rent, or trade your personal data to third parties.

We may share your information only in the following circumstances:

1. Service Providers

We work with trusted third-party vendors who help us deliver and improve our Services.

Below is a list of our service providers and their purposes:

Authentication & Identity

- **Clerk** – User authentication, session management, and account security. Data accessed: email, name, authentication tokens.

AI & Language Processing

- **Vercel AI Gateway** – Unified gateway for AI-powered features including accomplishment refinement, reflections, and goal insights. Routes requests to various AI model providers. Data accessed: user-submitted content for processing.

Analytics & Performance

- **PostHog** – Product analytics, feature usage tracking, and in-app surveys. Data accessed: usage behavior, device info, anonymized events.
- **Vercel Analytics** – Performance monitoring. Data accessed: page load times, web vitals.

Error Tracking & Monitoring

- **Sentry** – Error tracking, performance monitoring, and session replay. Data accessed: error logs, stack traces, masked session data.
- **Better Stack / Logtail** – Server log aggregation and uptime monitoring. Data accessed: server logs, request metadata.

Communications

- **Resend** – Transactional email delivery (reminders, notifications). Data accessed: email address, notification content.
- **Knock** – In-app notifications and notification preferences. Data accessed: user ID, notification content.

Infrastructure & Hosting

- **Vercel** – Application hosting, serverless functions, and edge network. Data accessed: all server-side data in transit.
- **Vercel Postgres** – Database hosting. Data accessed: all stored user data.
- **Vercel KV / Upstash** – Caching and rate limiting. Data accessed: session tokens, rate limit counters.

Payments (if applicable)

- **Stripe** – Payment processing and subscription management. Data accessed: payment method, billing address, transaction history.

Security

- **Arcjet** – Bot detection and attack prevention. Data accessed: request metadata, IP addresses.

2. Legal Requirements

We may disclose information when required by law, subpoena, court order, or other legal process, or when we believe disclosure is necessary to:

- Comply with applicable laws or regulations
- Respond to lawful requests from public authorities
- Protect the rights, property, or safety of Company, our users, or others
- Investigate or prevent potential security threats, fraud, or abuse

3. Business Transfers

In the event of a merger, acquisition, reorganization, bankruptcy, or sale of all or a portion of our assets, your information may be transferred as part of that transaction. We will notify you of any such change and any choices you may have regarding your information.

4. Aggregated or De-Identified Data

We may use and share aggregated or de-identified data that does not identify individual users for analytical, research, or marketing purposes.

V. Data Security

We implement appropriate technical and organizational security measures to protect your information:

- **Encryption in Transit**: All data encrypted in transit using TLS 1.2+
- **PII Encryption**: Personally identifiable information is encrypted at rest with AES-256-GCM
- **Secure Authentication**: Account protection via Clerk-managed sessions and passwordless authentication options
- **Access Controls**: Role-based access controls and authentication for all systems
- **Secure Storage**: Authentication secrets stored in platform keychains or secure enclaves
- **Regular Assessments**: Ongoing security monitoring and vulnerability assessments
- **Secure Infrastructure**: Data centers with physical security controls

Despite these safeguards, no method of transmission over the Internet or electronic storage is 100% secure. By using Olllo, you acknowledge and accept these inherent risks.

VI. Data Retention

We retain your information for as long as your account is active or as needed to provide Services. Our retention practices include:

- **Account and profile data** – Until account deletion + 30 days

- **User-generated content** – Until account deletion + 30 days
- **Consent records** – 7 years (legal compliance requirement)
- **Server logs** – 90 days
- **Anonymized analytics** – Indefinitely
- **Payment records** – As required by tax and financial regulations

Upon account deletion request:

- Personal data is removed within **30 days**
- Consent records are retained for **7 years** for legal compliance
- Anonymized or aggregated data may be retained indefinitely
- Backup systems are purged according to our backup rotation schedule

VII. Your Rights and Choices

1. Access and Portability

You can access and export your data through your account settings. We provide data export in standard formats (JSON/CSV).

2. Correction

You can update your account information and preferences at any time through your account settings.

3. Deletion

You can request deletion of your account and personal data by contacting privacy@olllo.ai. Deletion requests are processed within 30 days, subject to legal retention requirements.

4. Opt-Out of Communications

You can opt out of marketing or promotional emails at any time through your notification preferences or by clicking "unsubscribe" in any email. Essential transactional messages (such as security alerts or account confirmations) will still be sent as needed.

5. Cookie Preferences

You can manage cookie preferences through your browser settings. Note that disabling certain cookies may affect Service functionality.

VIII. California Privacy Rights (CCPA/CPRA)

If you are a California resident, you have additional rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA):

Your California Rights

- **Right to Know**: You may request information about the categories and specific pieces of personal information we have collected, the sources of collection, our business purposes, and categories of third parties with whom we share information.
- **Right to Delete**: You may request deletion of your personal information, subject to certain exceptions.
- **Right to Correct**: You may request correction of inaccurate personal information.
- **Right to Opt-Out of Sale/Sharing**: **We do not sell or share your personal information** for cross-context behavioral advertising. No opt-out is necessary.
- **Right to Limit Use of Sensitive Personal Information**: You may request that we limit our use of sensitive personal information to what is necessary to provide the Services.
- **Right to Non-Discrimination**: We will not discriminate against you for exercising your privacy rights.

Categories of Personal Information Collected

Under CCPA, we collect the following categories of personal information:

- **Identifiers** – Name, email, IP address, device IDs. Collected: Yes.
- **Personal Information (Cal. Civ. Code 1798.80)** – Name, employment information. Collected: Yes.
- **Protected Classifications** – None collected. Collected: No.
- **Commercial Information** – Subscription/purchase history. Collected: Yes (if applicable).
- **Internet/Network Activity** – Browsing history, interactions with Services. Collected: Yes.
- **Geolocation Data** – General location from IP address. Collected: Yes (approximate only).
- **Professional/Employment Information** – Job title, company, industry. Collected: Yes.
- **Inferences** – Preferences, characteristics from usage. Collected: Yes.
- **Sensitive Personal Information** – Account credentials. Collected: Yes (secured).

How to Exercise Your Rights

To exercise your California privacy rights, contact us at privacy@olllo.ai. We will verify your identity before processing your request. You may designate an authorized agent to make a request on your behalf.

IX. European Privacy Rights (GDPR)

If you are located in the European Economic Area (EEA), United Kingdom, or Switzerland, you have additional rights under the General Data Protection Regulation (GDPR):

Legal Basis for Processing

We process your personal data based on the following legal grounds:

- **Contract Performance**: Processing necessary to provide the Services you requested
- **Legitimate Interests**: Processing for our legitimate business interests (e.g., security, fraud prevention, service improvement) where not overridden by your rights
- **Consent**: Where you have given explicit consent for specific processing activities
- **Legal Obligation**: Processing necessary to comply with legal requirements

Your GDPR Rights

- **Right of Access**: Request a copy of your personal data
- **Right to Rectification**: Request correction of inaccurate data
- **Right to Erasure**: Request deletion of your data ("right to be forgotten")
- **Right to Restrict Processing**: Request limitation of processing in certain circumstances
- **Right to Data Portability**: Receive your data in a structured, machine-readable format
- **Right to Object**: Object to processing based on legitimate interests or for direct marketing
- **Right to Withdraw Consent**: Withdraw consent at any time where processing is based on consent
- **Right to Lodge a Complaint**: File a complaint with your local data protection supervisory authority

Automated Decision-Making

Our AI features assist in organizing and summarizing your professional information but do not make automated decisions with legal or similarly significant effects on you. You always retain control over how AI-generated content is used.

International Data Transfers

Your information may be transferred to and processed in countries other than your own, including the United States. When we transfer data outside the EEA/UK, we ensure appropriate safeguards are in place, including:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Data processing agreements with all service providers
- Compliance with applicable data protection frameworks

Data Protection Contact

For GDPR-related inquiries, contact us at privacy@olllo.ai.

X. Links to Other Websites

Our Services may contain links to third-party websites (for example, support documentation, partner sites, or social media).

We are not responsible for the content, privacy practices, or data collection of any linked third-party sites. We encourage you to review the privacy policies of any websites you visit through links on our Services.

XI. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors.

- **Significant updates** will be communicated via in-app notice or email at least **30 days** before taking effect.
- **Minor updates** (e.g., clarifications, formatting) take effect immediately upon posting.

You can always find the most current version at https://olllo.ai/privacy. The "Last Updated" date at the top indicates when this policy was last revised.
Your continued use of the Services after changes become effective constitutes acceptance of the revised Privacy Policy.

XII. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us:

Hypoth, Inc.

80 Piers Park Ln, Apt 3202 East Boston, MA 02128

Email: privacy@olllo.ai

Website: https://olllo.ai

For California residents: You may also contact us to exercise your CCPA rights.

For EU/EEA residents: You may contact us regarding GDPR rights or to lodge a complaint with your local supervisory authority.