

PRIVACY POLICY

EAG Inc.

nuEra Solutions™ — Land AI Assistant Platform

Effective Date: June 1, 2026 | Last Updated: June 1, 2026

1. INTRODUCTION

EAG Inc. (“**EAG**,” “**we**,” “**us**,” or “**our**”) is committed to protecting the privacy and security of you, either individually, or on behalf of your employer or any other entity which you represent. This Policy applies to all users of the Service, including individual users, Clients’ Administrators, and any person who visits our website or communicates with us (collectively, “**Client**”). By accessing or using the Service, each Client acknowledges that Client has read, understood, and agreed to the practices described in this Policy.

This Privacy Policy (“**Policy**”) describes how we collect, use, disclose, store, and protect information when Client accesses or uses the nuEra Solutions Land AI Assistant platform, including all related services, features, automation modules, tools, and outputs (collectively, the “**Service**”), visits our website, or otherwise interacts with us. EAG acts as a data processor/service provider with respect to Client documents. With respect to Client Documents and any personal information contained therein, EAG acts solely as a service provider or data processor on behalf of the Client and processes such data only in accordance with Client instructions.

This Privacy Policy should be read in conjunction with our [Terms of Service](#), which govern the use of the Service and are incorporated herein by reference. In the event of any conflict between this Privacy Policy and the Terms of Service, the Terms of Service shall control with respect to legal terms, liability, and dispute resolution, while this Privacy Policy shall control with respect to disclosures regarding how personal information is collected, used, retained, and handled. Capitalized terms used but not defined in this Privacy Policy have the meanings assigned to them in the Terms of Service.

2. INFORMATION WE COLLECT

We collect information in the following categories:

2.1 Information Users Provide Directly

- **Account Registration Information.** When a User creates an account, we collect User’s name, email address, Client name, job title, phone number, and other information User provides during registration.
- **Billing Information.** If a User subscribes to a paid plan, we collect payment-related information such as billing address and payment method details. Payment card information is processed by our third-party payment processor and is not stored on our servers.
- **Client Documents.** Users may upload documents in PDF or other supported formats to the Service for AI-powered processing. The handling of Client Documents is described in detail in Section 5 (Data Retention and Storage) herein.
- **User Prompts and Instructions.** When using the Service, a User may provide prompts, queries, custom instructions, or other input directing the AI tools to perform specific tasks.

- **Communications.** When a User contacts us for support, provides feedback, or otherwise communicates with us, we collect the content of those communications.

2.2 Information Collected Automatically

- **Usage Data.** We automatically collect information about how Clients interact with the Service, including timestamps, automation modules used, document counts processed, processing durations, features accessed, and other operational telemetry.
- **Device and Browser Information.** We may collect information about the device and browser Clients use to access the Service, including IP address, browser type and version, operating system, device identifiers, and screen resolution.
- **Log Data.** Our servers automatically record information when Clients access the Service, including each Client's IP address, the date and time of Client's request, the pages or features accessed, and referring URLs.
- **Cookies and Similar Technologies.** We use cookies and similar tracking technologies to maintain session state, remember Clients' preferences, and analyze Service usage. See Section 10 (Cookies and Tracking Technologies) herein for more information.

2.3 Information from Third Parties

We may receive information about Clients from third parties, including identity verification services, business information providers, and referral partners, solely for the purposes of verifying a Client's identity, preventing fraud, or facilitating Clients' use of the Service.

3. HOW WE USE USERS' INFORMATION

We use the information we collect for the following purposes:

3.1 Providing and Improving the Service

- Processing Client Documents through the AI automation modules as directed by Clients;
- Generating Output in response to Clients' requests;
- Maintaining and administering Clients' accounts;
- Processing payments and managing subscriptions;
- Providing customer support and responding to inquiries;
- Monitoring Service performance, reliability, and uptime; and
- Identifying and resolving technical issues, bugs, and errors.

3.2 Security and Compliance

- Detecting, investigating, and preventing fraud, unauthorized access, and other security threats;
- Enforcing our Terms of Service and other agreements;
- Complying with applicable legal obligations, including regulatory requirements, court orders, and lawful requests from governmental authorities; and
- Protecting the rights, safety, and property of EAG, Clients, and the public.

3.3 Communications

- Sending service-related notifications, including account alerts, security notices, maintenance updates, and billing information;
- Responding to Clients' requests, questions, and feedback; and
- With Clients' consent, sending promotional communications about new features, products, or services. Clients may opt out of promotional communications at any time.

3.4 Analytics

- Analyzing usage patterns and trends to improve the Service;
- Generating aggregate, de-identified statistics about Service usage; and
- Conducting internal research and development to enhance our AI tools and automation capabilities.

3.5 What We Do NOT Use Client Information For

Except as otherwise disclosed in this Policy or required by applicable law, we do **not** use Clients' information for the following purposes:

- **No AI model training.** Client Documents, Output, and Client prompts are not used to train, fine-tune, or improve general-purpose artificial intelligence or machine learning models;
- **No behavioral profiling.** We do not build behavioral profiles of individual Clients for advertising, marketing, or other commercial purposes unrelated to the Service;
- **No selling of Client data.** We do not sell, rent, or trade Clients' personal information or Client Documents to third parties; and
- **No targeted advertising.** We do not use Clients' information to serve third-party targeted advertisements.

4. THIRD-PARTY AI SERVICE PROVIDERS

4.1 How Client Data Is Processed

The Service utilizes third-party artificial intelligence infrastructure providers ("**AI Providers**") to process Client Documents and generate Output. When a Client submits Client Documents or prompts to the Service, such Client data may be transmitted to and processed by one or more AI Providers as part of the automation workflow.

4.2 Data Protections

We select AI Providers that maintain commercially reasonable data protection standards. With respect to Client data processed through AI Providers:

- All data transmitted to AI Providers is encrypted in transit using HTTPS/SSL/TLS protocols;
- EAG requires AI Providers, through contractual obligations, to restrict their use of Client Documents, Output, or Client prompts to train, fine-tune, or improve their own general-purpose models or any third-party models;
- AI Providers operate as independent service providers and are not agents or representatives of EAG. While we impose contractual restrictions on AI Providers, we do not control their operations and cannot guarantee their compliance.
- AI Providers process Client's/Clients' data solely for the purpose of generating the requested Output and are contractually required not to retain Client's/Clients' data beyond what is necessary for immediate processing. Any transient retention by AI Providers for purposes such as abuse monitoring or system integrity is subject to their data processing agreements and is limited in duration and scope;
- AI Providers are bound by data processing agreements that require compliance with applicable data protection laws; and
- We periodically review AI Provider practices to ensure ongoing compliance.

While we require AI Providers to adhere to strict data handling standards, we cannot guarantee their compliance and disclaim any liability for AI Provider's independent actions.

5. DATA RETENTION AND STORAGE

5.1 Default Zero Data Retention

For clarity, our zero-retention policy applies only to Client Documents and Output and does not apply to Metadata or Prompt Data as described below. By default, the Service operates under a strict **Zero Data Retention** policy for Client Documents and Output. Transient processing may include temporary caching, buffering, secure queueing, infrastructure replication, and other technical operations reasonably necessary to provide the Service. For the avoidance of doubt, 'Zero Data Retention' refers to the absence of persistent storage within EAG-controlled systems following completion of processing, and does not preclude transient processing, temporary storage, or limited retention required for system integrity, security, or legal compliance. This means:

- Client Documents are stored only in a temporary environment during the active automation session;
- Output is generated and made available to the Client for download or export during the session;
- Once the session ends or the automation task is completed, Client Documents and Output are permanently deleted from our systems; and
- Clients must export or download Output before ending their session, as data will not be recoverable afterward.

5.2 Administrator-Enabled Data Retention

Each Client's Administrator may override the default zero-retention policy by enabling the "**Save Automation Data**" toggle in the Client's account settings. When enabled:

- **Scope.** All automation result data and associated metadata are retained within the Service.
- **Duration.** Retained data is stored for up to ninety (90) days from the date of processing unless deleted earlier by a Client Administrator. Following expiration of the retention period, retained data is permanently deleted from the active database. Automated database backups may retain such data for up to fourteen (14) additional calendar days before permanent purge.
- **Deletion.** Deleted data is permanently removed from the active database. Automated database backups may retain the data for up to fourteen (14) calendar days after deletion, after which it is permanently purged.
- **Administrator Responsibility and In-Product Indicators.** We provide in-product indicators that display the current data retention status within the Service interface. Each Client's Administrator bears primary responsibility for communicating data retention policies to Client end users within the Client organization. We encourage Client' Administrators to notify all Client end users promptly when data retention settings are changed.
- **Legal Compliance.** Retained data is processed solely in accordance with Client instructions and applicable data protection laws.

5.3 Temporary Data Processing

Certain long-running or complex automations require temporary storage to ensure task completion. In these cases:

- Data is held in a secure, isolated environment;
- Temporary data is automatically purged within twenty-four (24) hours of task completion;

- Temporary data is not included in any database backup or archival process;
- Access is restricted to automated processing systems only; and
- Temporary storage is never used for profiling, analytics, advertising, or model training.

5.4 Metadata and Prompt Data

For clarity, our zero-retention policy applies only to Client Documents and Output and does not apply to Metadata or Prompt Data as described below. Notwithstanding the zero-retention policy, we retain and control **Metadata** as necessary to operate, secure, and improve the Service, as described in the Terms of Service Policy and this Policy. As used in this Policy, Metadata includes:

- **Prompt Data** — the text of Client-submitted prompts, queries, and instructions (does not include the content of Client Documents). Prompt Data is used solely for purposes of operating, maintaining, securing, and improving the performance and reliability of the Service, and is not used to train general-purpose artificial intelligence models;
- **Usage Data** — timestamps, document counts, module usage, processing durations, and other operational telemetry;
- **Account Data** — Client identification, login activity, role assignments, and Client association; and
- **System Data** — error logs, performance metrics, and technical diagnostics.

5.5 Account Information

Account registration information and billing records are retained for the duration of the account relationship and for a reasonable period thereafter as necessary to comply with legal obligations, resolve disputes, and enforce our agreements.

6. HOW WE SHARE CLIENT INFORMATION

We do not sell Clients' personal information as those terms are defined under applicable data protection laws, including the California Consumer Privacy Act (CCPA/CPRA). We may share a Client's information in the following limited circumstances:

6.1 Service Providers and AI Providers

We engage trusted third-party service providers to assist in delivering the Service, including cloud hosting providers, AI infrastructure providers (as described in Section 4 herein), payment processors, analytics providers, and customer support tools. These providers are contractually obligated to protect the confidentiality of Client information and may only process it as directed by us.

6.2 Legal Requirements

We may disclose a Client's information if required to do so by applicable law, regulation, legal process, or governmental request, including in response to court orders, subpoenas, or requests from regulatory authorities.

6.3 Protection of Rights

We may disclose a Client's information where we believe disclosure is necessary to: (a) enforce our Terms of Service or other agreements; (b) protect the rights, safety, or property of EAG, Clients, or the public; (c) detect, prevent, or address fraud, security issues, or technical problems; or (d) respond to an emergency involving danger of death or serious physical injury.

6.5 With Client's Consent

We may share a Client's information for any other purpose with a Client's explicit consent.

6.6 Aggregate and De-Identified Data

We may share aggregate or de-identified information that cannot reasonably be used to identify a Client for any purpose, including industry benchmarking, research, and marketing.

7. DATA SECURITY

We implement and maintain commercially reasonable administrative, technical, and organizational security measures designed to protect Client information from unauthorized access, disclosure, alteration, and destruction. These measures include:

- **Encryption in Transit.** All data transmitted between a Client browser and our servers is encrypted using HTTPS/SSL/TLS protocols.
- **Multi-Factor Authentication.** Multi-factor authentication (MFA) is available and strongly encouraged for all Client accounts. MFA requirements may vary based on account type and subscription tier.
- **Access Controls.** Role-based access controls limit our personnel access to Client data on a need-to-know basis.
- **Infrastructure Security.** The Service is hosted on secure cloud infrastructure provided by reputable third-party providers with industry-standard certifications.
- **Monitoring.** We conduct regular security assessments, vulnerability scanning, and monitoring of our systems.
- **Incident Response.** We maintain incident response procedures to promptly address any security event.
- **Data Residency.** Client data processed through the Service, including Client Documents, Output (if retained), and Metadata, is primarily hosted and processed within the United States using U.S.-based cloud infrastructure. Notwithstanding the foregoing, data processed through the Service may be accessed by authorized personnel or providers in other jurisdictions. We do not intentionally transfer or store such data outside of the United States. To the extent that any data is accessed by authorized personnel or service providers, such access is conducted in accordance with applicable data protection laws and appropriate contractual safeguards.

We reserve the right to adjust each of the above data security measures as appropriate based on the nature of the Service. While we employ commercially reasonable security measures, no method of electronic transmission or storage is completely secure. We cannot guarantee absolute security, and Clients use the Service at their own risk. While we implement commercially reasonable safeguards, such measures are not guaranteed to prevent all unauthorized access or breaches.

8. COOKIES AND TRACKING TECHNOLOGIES

8.1 What We Use

We use cookies and similar technologies to operate and improve the Service. The types of cookies we use include:

- **Essential Cookies.** Required for the Service to function properly, including session management, authentication, and security. These cookies cannot be disabled.
- **Functional Cookies.** Remember Clients' preferences and settings to provide a personalized experience.

- **Analytics Cookies.** Help us understand how Clients interact with the Service so we can improve functionality and performance. Analytics data is collected in aggregate form.

9. CLIENTS' RIGHTS AND CHOICES

For clarity, the rights set forth in this Section shall apply only where required by applicable law. Depending on applicable law, Clients may have the following rights:

9.1 Access and Portability

A Client may request confirmation of whether we process the Client's personal information and obtain a copy of that information in a structured, commonly used, machine-readable format.

9.2 Correction

A Client may request correction of inaccurate or incomplete personal information. A Client can also update the Client's account information directly through the Service.

9.3 Deletion

A Client may request deletion of Client's personal information, subject to certain exceptions. We may retain information as required by law, to complete a transaction, for legitimate business purposes, or as otherwise permitted by applicable law. Note that Client Documents and Output are automatically deleted under our zero-retention policy (Section 5.1 herein) unless data retention has been enabled by a Client's Administrator for the Client.

9.4 Restriction of Processing

A Client may request that we restrict the processing of Client's personal information under certain circumstances, such as when a Client contests the accuracy of the data or objects to our processing.

9.5 Objection

Where we process personal Client information based on legitimate interests, a Client may object to such processing. Upon receiving Client's objection, we will cease processing unless we can demonstrate compelling legitimate grounds that override a Client's interests.

9.6 Withdrawal of Consent

Where processing is based on a Client consent, such Client may withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing conducted prior to withdrawal.

9.7 Non-Discrimination

We will not discriminate against a Client for exercising any Client privacy rights. A Client will not receive different pricing, a different quality of service, or be denied access to the Service for exercising a Client rights.

9.8 How to Exercise Client Rights

To exercise any of these rights, please contact us using the information provided in Section 17 (Contact Information) here. We will respond to verified requests within the timeframes required by applicable law. We may require verification of a Client's identity before processing a request.

10. GEOGRAPHIC RESTRICTIONS

This Service is intended solely for Clients located within the United States of America. By accessing or using this Service, a Client represents and warrants that the Client is physically located in, and accessing

the Service from within, the United States. Clients located outside the United States are not authorized to access or use this Service. We reserve the right to restrict, suspend, or terminate access to the Service for any Client we reasonably believe is accessing the Service from outside the United States, without prior notice or liability.

We make no representation that the Service is appropriate, available, or legally permissible for use in any jurisdiction outside the United States. If a Client accesses the Service from outside the United States, such Client does so at such Client's own risk and are solely responsible for compliance with applicable local laws.

We may expand availability to additional regions in the future at our sole discretion.

11. DATA PROCESSING AGREEMENTS

For Clients subject to data protection laws that require a formal data processing agreement, we will enter into a Data Processing Agreement ("DPA") upon written request. The DPA will address the categories of personal data processed, the purposes of processing, our obligations as a data processor, data breach commitments, international data transfer mechanisms, and audit cooperation obligations.

To request a DPA, please contact us at legal@eaginc.com. We will provide a standard DPA template within a reasonable timeframe.

12. CHILDREN'S PRIVACY

The Service is designed for business use and is not directed to individuals under the age of 18. We do not knowingly collect personal information from individuals under the age of 18 years old. If we become aware that we have inadvertently collected personal information from an individual under the age of 18 years old, we will take reasonable steps to promptly delete such information. If someone believes that an individual under the age of 18 years old has provided us with personal information, please contact us immediately using the contact information provided in Section 17 herein.

13. CONTACT INFORMATION

If a Client has any questions, concerns, or requests regarding this Privacy Policy or our data practices, wish to request a Data Processing Agreement, or wish to exercise any of Client's rights under applicable data protection law, please contact us at:

EAG Inc.

Email: legal@eaginc.com

We will endeavor to respond to all inquiries within a reasonable time and in accordance with applicable law.

14. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or for other operational reasons. When we make material changes, we will:

- Post the updated Policy on our website with a revised "Last Updated" date;
- Notify registered Clients via email or through an in-app notification; and

- Where required by applicable law, obtain a Client’s consent before implementing material changes.

We encourage each Client to review this Policy periodically. A Client’s continued use of the Service after any changes constitutes such Client’s acceptance of the updated Policy.

15. CLIENT’S COMPLIANCE WITH LAW

Client is solely responsible for ensuring that each of its Clients has all necessary rights, consents, and legal authority to collect, use, process, and submit Client Documents, personal information, and any other data to the Service. We do not verify the legality of Client Documents or other data submitted by Clients and disclaims any responsibility for the lawfulness, accuracy, or appropriateness of such data. Client is responsible for its Client end users complying with all applicable data protection, privacy, and other laws in connection with Client use of the Service.

16. LIMITATION OF LIABILITY

This Policy is incorporated into and forms part of the Terms of Service governing each Client’s use of the Service. To the maximum extent permitted by applicable law, any limitations of liability, disclaimers, and exclusions set forth in the Terms of Service shall apply to our collection, use, disclosure, and handling of information as described in this Privacy Policy.

17. DATA RETENTION SUMMARY

The following table summarizes our data retention practices for ease of reference:

DATA TYPE	RETAINED?	DURATION	BACKED UP?
CLIENT DOCUMENTS	NO (DEFAULT)	DELETED AFTER SESSION	NO
OUTPUT	NO (DEFAULT)	DELETED AFTER SESSION	NO
SAVED AUTOMATION DATA	IF ENABLED BY ADMIN	90 DAYS FROM PROCESSING DATE	YES (14-DAY BACKUP)
TEMPORARY PROCESSING DATA	TRANSIENT ONLY	PURGED WITHIN 24 HOURS	NO
PROMPT DATA	YES	90 DAYS	YES (14-DAY PURGE AFTER EXPIRY)
USAGE METADATA	YES	AS LONG AS NECESSARY (PERIODIC REVIEW)	YES
ACCOUNT INFORMATION	YES	DURATION OF ACCOUNT + POST-TERMINATION PERIOD	YES
BILLING RECORDS	YES	AS REQUIRED BY LAW	YES
AI PROVIDER PROCESSING	NO	NOT RETAINED BY AI PROVIDERS	NO

For detailed information about each data category’s controlling terms, please refer to Section 5 (Data Retention and Storage) herein and the corresponding sections of our Terms of Service.