

Privacy Policy

Effective Date: 6 July 2026

Last Updated: 6 July 2026

Version: 1.0

1. Introduction

Welcome to ServeusAI.

At ServeusAI, we recognize that privacy and the responsible handling of personal information are fundamental to building trust with our Customers, users and business partners. This Privacy Policy explains how ServeusAI collects, uses, discloses, stores and protects Personal Data when individuals interact with our websites, products and services, including the Minerva platform.

This Privacy Policy has been prepared in accordance with the requirements of the General Data Protection Regulation (EU) 2016/679 ("GDPR") and other applicable data protection laws.

The purpose of this Policy is to provide transparent information regarding:

- what Personal Data we collect;
- why we collect it;
- how we use it;
- when we share it;
- how long we retain it;
- how we protect it; and
- the rights available to individuals under applicable data protection laws.

Where ServeusAI processes Personal Data on behalf of Customers through the Minerva platform, ServeusAI generally acts as a **Data Processor**, while the Customer acts as the **Data Controller**.

Where ServeusAI collects Personal Data directly—for example through our website, contact forms, sales enquiries, customer support or contractual relationships—ServeusAI acts as the **Data Controller**.

This distinction is important because the rights and responsibilities of each party differ depending on the context of the processing activity.

2. Scope

This Privacy Policy applies to Personal Data processed through:

- the ServeusAI corporate website;
- the Minerva web application;
- customer and prospect communications;
- sales and onboarding activities;
- customer support services;
- contractual relationships;
- marketing communications where applicable;
- security and compliance activities;
- cookies and analytics technologies; and
- any other services operated by ServeusAI that reference this Privacy Policy.

This Privacy Policy does **not** apply to the processing of Personal Data performed solely under the instructions of Customers within the Minerva platform.

Such processing is governed by the applicable **Data Processing Agreement (DPA)** entered into between ServeusAI and the Customer.

3. Privacy Principles

ServeusAI's privacy program is based upon the following principles.

Lawfulness, Fairness and Transparency

We process Personal Data only where an appropriate legal basis exists and provide clear information regarding our processing activities.

Purpose Limitation

Personal Data is collected only for specified, explicit and legitimate purposes and is not further processed in a manner incompatible with those purposes.

Data Minimization

We seek to collect only the Personal Data that is necessary for the relevant purpose.

Accuracy

Reasonable efforts are made to ensure that Personal Data remains accurate and up to date.

Storage Limitation

Personal Data is retained only for as long as necessary to fulfil the purposes for which it was collected or as otherwise required by applicable law.

Integrity and Confidentiality

Appropriate technical and organizational measures are implemented to protect Personal Data against unauthorized access, accidental loss, alteration or disclosure.

Accountability

ServeusAI continuously reviews and improves its privacy and security practices and maintains documentation demonstrating compliance with applicable data protection requirements.

This Privacy Policy should be read together with the following documents where applicable:

- Terms of Service;
- Data Processing Agreement (DPA);
- Security Overview;
- Cookie Policy; and
- Approved Subprocessor List.

4. Data Controller

Who We Are

This Privacy Policy is issued by **ServeusAI Kft.** ("ServeusAI", "we", "our" or "us").

ServeusAI develops and operates the Minerva platform and provides related products and services to business customers.

Depending on the nature of the processing activity, ServeusAI may act either as a **Data Controller** or as a **Data Processor** under the General Data Protection Regulation (GDPR).

When ServeusAI Acts as a Data Controller

ServeusAI acts as the **Data Controller** when we determine the purposes and means of processing Personal Data.

This generally includes Personal Data processed in connection with:

- visits to the ServeusAI website;
- enquiries submitted through contact forms;
- requests for demonstrations of the Services;
- communication with prospective Customers;
- customer account administration;
- contractual relationships;
- invoicing and payment administration;
- customer support communications;
- compliance activities;
- security monitoring;
- marketing communications where consent has been provided or another lawful basis exists; and
- recruitment activities, where applicable.

For these processing activities, ServeusAI is responsible for ensuring compliance with applicable data protection legislation.

When ServeusAI Acts as a Data Processor

When Customers use the Minerva platform to upload, store, analyze or otherwise process documents containing Personal Data, ServeusAI generally acts solely as a **Data Processor**.

In these circumstances:

- the Customer determines the purposes of processing;
- the Customer determines the categories of Personal Data processed;
- the Customer determines the legal basis for processing;
- the Customer remains responsible for responding to Data Subject requests; and
- ServeusAI processes Personal Data only on documented instructions from the Customer.

The relationship between ServeusAI and its Customers is governed by the applicable **Data Processing Agreement (DPA)**.

Categories of Individuals

Depending on the circumstances, Personal Data may relate to:

- website visitors;
- prospective Customers;
- customer representatives;
- authorized users of the Minerva platform;
- suppliers and business partners;

- support contacts;
- billing contacts; and
- other individuals whose Personal Data is included within Customer Content uploaded to the Services.

For Personal Data contained within Customer Content, the relevant Customer remains responsible for ensuring that such processing complies with applicable laws.

Contact Details

For questions relating to this Privacy Policy or the processing of Personal Data, you may contact ServeusAI using the contact information published on our website.

Privacy-related enquiries may include:

- requests regarding Personal Data;
- questions concerning this Privacy Policy;
- requests relating to GDPR rights;
- security or privacy concerns; and
- complaints regarding the processing of Personal Data.

ServeusAI will respond to requests within the timeframes required by applicable law.

Data Protection Officer

At the time of publication of this Privacy Policy, ServeusAI has **not appointed a formal Data Protection Officer (DPO)**.

Privacy compliance responsibilities are managed internally by designated personnel responsible for information security, privacy and regulatory compliance.

Should the appointment of a Data Protection Officer become legally required or operationally appropriate, this Privacy Policy will be updated accordingly.

Supervisory Authority

If you believe that the processing of your Personal Data infringes applicable data protection laws, you have the right to lodge a complaint with the competent supervisory authority in your country of residence, place of work or the location of the alleged infringement.

Where appropriate, we encourage individuals to contact ServeusAI first so that we may have the opportunity to address any concerns directly and efficiently.

Changes to Controller Information

ServeusAI may update its corporate information, contact details or organizational structure from time to time.

Any material changes affecting the identity of the Data Controller or the manner in which Personal Data is processed will be reflected in an updated version of this Privacy Policy.

5. Personal Data We Collect

Overview

The categories of Personal Data processed by ServeusAI depend on how individuals interact with our websites, products and services.

We collect Personal Data directly from individuals, automatically through the use of our Services and, in certain circumstances, from our Customers or trusted third-party service providers.

We seek to collect only the information necessary to provide, secure and improve our Services, fulfil contractual obligations and comply with applicable legal requirements.

Information You Provide Directly

Individuals may voluntarily provide Personal Data when interacting with ServeusAI.

Examples include:

- name;
- business email address;
- company name;
- job title;
- telephone number;
- billing information;
- account credentials;
- communications with our team;
- support requests;
- feedback;
- information submitted through contact forms; and
- information provided when requesting a product demonstration.

Providing certain information may be necessary to establish or maintain a contractual relationship with ServeusAI.

Account Information

When an organization creates a Minerva account, we may process information relating to authorized users, including:

- name;
- business email address;
- organization;
- user role;
- authentication information;
- account status;
- language preferences;
- login history;
- user preferences; and
- account activity necessary to provide the Services.

This information is used to authenticate users, manage access and administer the platform.

Customer Content

Customers may upload documents and other information to the Minerva platform for processing.

Depending on how the platform is used, Customer Content may include:

- contracts;
- invoices;
- purchase orders;
- certificates;
- reports;
- presentations;
- spreadsheets;
- email attachments;
- identity documents;
- HR-related documents;
- technical documentation;
- compliance documentation; and
- other business records selected by the Customer.

Customer Content may contain Personal Data.

ServeusAI does not determine the categories of Personal Data contained within Customer Content. Customers are responsible for deciding what information is uploaded to the Services and for ensuring that such processing complies with applicable law.

AI Processing Data

When Customers choose to use AI-assisted functionality, Minerva may process information necessary to perform the requested operation.

Depending on the selected feature, this may include:

- prompts;
- document text;
- extracted information;
- document fragments;
- metadata required for processing; and
- AI-generated responses.

This information is processed solely for the purpose of providing the requested AI functionality.

Additional information regarding AI processing is provided in our Security Overview and Data Processing Agreement.

Automatically Collected Information

When individuals access our websites or use the Minerva platform, certain technical information may be collected automatically.

This may include:

- IP address;
- browser type;
- operating system;
- device information;
- language settings;
- pages visited;
- referring URLs;
- session information;
- timestamps;
- application usage statistics;
- error reports; and
- diagnostic information.

This information helps us maintain the security, availability and performance of our Services.

Cookies and Similar Technologies

ServeusAI uses cookies and similar technologies to support the operation of its websites and Services.

Depending on the applicable website functionality and user consent, ServeusAI uses **Strictly Necessary Cookies, Preference Cookies and Analytics Cookies** as described in the Cookie Policy.

Cookie preferences are managed using **Usercentrics Consent Management Platform (CMP)**.

Further information is available in our Cookie Policy.

Analytics Information

Where permitted by applicable law and user consent, ServeusAI uses analytics technologies to better understand how visitors interact with our websites.

Analytics technologies currently include:

- Google Analytics; and
- Google Tag Manager.

Analytics information is used to:

- understand website traffic;
- improve website usability;
- identify technical issues;
- measure feature adoption; and
- improve the overall user experience.

Analytics data is used in aggregated form wherever reasonably practicable.

Customer Support Information

When Customers contact our support team, we may process information necessary to investigate and resolve the reported issue.

This may include:

- contact information;

- organization details;
- support communications;
- technical logs;
- screenshots provided by the Customer;
- diagnostic information;
- support tickets; and
- information voluntarily provided during the support process.

ServeusAI personnel access Customer Content only where necessary to provide support and, whenever practical, with the Customer's authorization.

Information from Third Parties

ServeusAI may receive limited Personal Data from trusted third parties, including:

- business partners;
- payment providers;
- technology service providers;
- publicly available business sources; and
- organizations that introduce prospective Customers.

Such information is processed only where there is an appropriate legal basis.

Information We Do Not Intentionally Collect

ServeusAI does not intentionally collect:

- information from children under the age required by applicable law;
- special categories of Personal Data unless submitted by Customers through the Services;
- Personal Data for advertising profiling; or
- Personal Data unrelated to the provision of our Services.

Customers remain responsible for determining whether the information they upload to Minerva is appropriate for processing.

Data Minimization

ServeusAI seeks to limit the collection of Personal Data to what is necessary for identified business purposes.

We periodically review our data collection practices to ensure that unnecessary information is not collected or retained beyond what is reasonably required.

Summary

The categories of Personal Data processed by ServeusAI vary depending on the relationship with the individual and the Services being used.

Information is collected only to the extent necessary to provide, secure and improve the Services, fulfil contractual obligations, support Customers and comply with applicable legal requirements.

6. How We Use Personal Data

Overview

ServeusAI processes Personal Data only where there is a legitimate business purpose and an appropriate legal basis under applicable data protection laws.

The purposes for which Personal Data is processed depend on the nature of the relationship between the individual and ServeusAI, as well as the Services being used.

We do not use Personal Data for purposes that are incompatible with those described in this Privacy Policy.

Providing the Services

The primary purpose of processing Personal Data is to provide and maintain the Minerva platform and related services.

This includes processing necessary to:

- create and manage user accounts;
- authenticate users;
- provide access to the Services;
- process Customer Content;
- generate AI-assisted outputs;
- maintain user preferences;
- provide requested functionality; and
- ensure the availability of the Services.

Without processing this information, we would be unable to provide the requested Services.

Customer Relationship Management

We process Personal Data to establish and manage our business relationships with Customers and prospective Customers.

This includes:

- responding to enquiries;
 - scheduling demonstrations;
 - preparing quotations;
 - negotiating contracts;
 - managing customer onboarding;
 - maintaining customer records;
 - communicating regarding the Services; and
 - administering commercial relationships.
-

Customer Support

Personal Data may be processed to provide technical support and customer assistance.

Support activities may include:

- responding to support requests;
- troubleshooting technical issues;
- investigating reported incidents;
- resolving account problems;
- communicating service updates;
- maintaining support records; and
- improving customer support processes.

Where access to Customer Content is required to resolve a support request, such access is limited to what is reasonably necessary.

Service Security

ServeusAI processes Personal Data to protect the confidentiality, integrity and availability of its Services.

Security-related processing may include:

- user authentication;
- fraud prevention;
- access management;
- monitoring security events;
- detecting unauthorized activity;
- vulnerability management;
- incident response;
- operational logging; and
- compliance monitoring.

These activities help protect both our Customers and the Services against security threats.

Operating and Improving the Services

We continuously evaluate and improve our products and services.

Personal Data may be processed to:

- improve platform performance;
- enhance usability;
- identify software defects;
- improve reliability;
- optimize system performance;
- develop new features;
- evaluate product usage; and
- improve the overall customer experience.

Where reasonably practicable, aggregated or anonymized information is used for analytical purposes.

AI-Assisted Functionality

When Customers choose to use AI-powered features, Personal Data may be processed to provide the requested functionality.

Depending on the selected feature, processing may include:

- document analysis;
- information extraction;
- summarization;
- question answering;
- classification;
- document comparison; and
- other AI-assisted capabilities available within Minerva.

ServeusAI processes Customer Content only for the purpose of delivering the requested AI functionality.

Communications

ServeusAI may use Personal Data to communicate with Customers and users regarding the Services.

Communications may include:

- account notifications;
- security alerts;
- service announcements;
- product updates;
- contractual communications;
- responses to enquiries;
- customer support communications; and
- other operational notices.

These communications are considered necessary for the operation of the Services.

Compliance with Legal Obligations

ServeusAI may process Personal Data where necessary to comply with applicable legal obligations.

Examples include:

- accounting requirements;
- tax obligations;
- regulatory reporting;
- responding to lawful requests from public authorities;
- legal proceedings;
- enforcement of contractual rights; and
- compliance with applicable laws and regulations.

Processing for these purposes occurs only where required or permitted by law.

Marketing Communications

Where permitted by applicable law, ServeusAI may send marketing communications regarding products, services, events or other business-related information.

Marketing communications are sent:

- where consent has been obtained; or
- where another lawful basis exists under applicable law.

Recipients may withdraw their consent or unsubscribe from marketing communications at any time.

Operational or contractual communications will continue where necessary, even if marketing communications are declined.

Website Analytics

Subject to applicable consent requirements, Personal Data may be processed to understand how visitors interact with our website.

This processing helps us:

- understand visitor behaviour;
- improve website performance;
- optimize navigation;
- evaluate content effectiveness;
- identify technical issues; and
- enhance the user experience.

Analytics processing is performed using approved service providers as described in this Privacy Policy and the Cookie Policy.

Business Operations

ServeusAI may process Personal Data to support its internal business operations.

Examples include:

- financial administration;
- supplier management;
- audit preparation;
- compliance activities;
- information security management;
- business continuity planning;
- internal reporting; and
- corporate governance.

Processing is limited to purposes necessary for the effective operation of the organization.

What We Do Not Use Personal Data For

ServeusAI does not use Personal Data to:

- sell Personal Data to third parties;
- build advertising profiles;
- deliver behavioural advertising based on Customer Content;
- train proprietary AI foundation models using Customer Content;
- develop commercial datasets from Customer Content; or
- use Customer Content for purposes unrelated to providing the Services.

Customer information remains under the control of the Customer, subject to the applicable contractual agreements.

Purpose Limitation

If ServeusAI intends to process Personal Data for a purpose materially different from those described in this Privacy Policy, we will update this Privacy Policy or otherwise provide appropriate notice where required by applicable law.

Summary

ServeusAI processes Personal Data only for legitimate, specified and transparent purposes related to providing, securing, supporting and improving the Services, fulfilling contractual obligations and complying with applicable legal requirements.

We are committed to ensuring that Personal Data is processed responsibly, proportionately and in accordance with applicable data protection laws.

7. Legal Bases for Processing

Overview

ServeusAI processes Personal Data only where a valid legal basis exists under the General Data Protection Regulation (GDPR) and other applicable data protection laws.

The legal basis depends on the specific purpose for which Personal Data is processed. In many cases, more than one legal basis may apply to a particular processing activity.

Performance of a Contract

The majority of Personal Data processed in connection with the Minerva platform is processed because it is necessary to perform a contract or to take steps prior to entering into a contract.

This legal basis applies to activities including:

- creating and managing customer accounts;
- authenticating users;
- providing access to the Services;
- processing Customer Content;
- delivering AI-assisted functionality;
- providing customer support;
- managing subscriptions;
- processing payments and invoicing; and
- fulfilling contractual obligations.

Without processing this information, ServeusAI would be unable to provide the Services requested by the Customer.

Legitimate Interests

ServeusAI may process Personal Data where such processing is necessary for our legitimate business interests, provided that those interests are not overridden by the rights and freedoms of the individual.

Examples include:

- improving the Services;
- maintaining platform security;
- fraud prevention;
- network and information security;
- responding to customer enquiries;
- business administration;
- supplier management;
- service monitoring;
- internal reporting;
- risk management;
- compliance monitoring; and
- defending legal claims.

Where processing is based on legitimate interests, ServeusAI considers the potential impact on individuals and implements appropriate safeguards.

Compliance with Legal Obligations

Certain Personal Data is processed because ServeusAI is required to comply with applicable legal obligations.

Examples include:

- accounting requirements;
- tax obligations;
- financial recordkeeping;
- responding to lawful requests from competent authorities;
- compliance with court orders;
- regulatory reporting;
- sanctions screening where applicable; and
- maintaining records required by law.

Where processing is required by law, the applicable legal obligation serves as the legal basis.

Consent

For certain processing activities, ServeusAI relies on the individual's consent.

Examples include:

- optional marketing communications;
- non-essential cookies;
- website analytics where consent is required; and
- similar optional processing activities.

Where consent is the legal basis:

- consent may be withdrawn at any time;
- withdrawal does not affect processing carried out before consent was withdrawn; and
- individuals are provided with appropriate mechanisms to manage their preferences.

Cookie preferences can be managed through the Usercentrics Consent Management Platform.

Protection of Vital Interests

In exceptional circumstances, ServeusAI may process Personal Data where necessary to protect the vital interests of an individual or another natural person.

Such situations are expected to be rare and will generally arise only where immediate action is necessary to protect life or prevent serious harm.

Public Interest

ServeusAI does not generally process Personal Data in the performance of tasks carried out in the public interest or in the exercise of official authority.

Should such processing become relevant in the future, this Privacy Policy will be updated accordingly.

Customer Content Processed on Behalf of Customers

When Customers use the Minerva platform to process Personal Data contained within uploaded documents, ServeusAI generally acts solely as a **Data Processor**.

In these circumstances:

- the Customer determines the legal basis for processing;
- the Customer determines the purposes of processing;
- the Customer determines the categories of Personal Data processed; and
- ServeusAI processes the information only on documented instructions from the Customer.

Individuals wishing to exercise their GDPR rights regarding Customer Content should normally contact the relevant Customer acting as Data Controller.

AI Processing

Where Customers choose to use AI-assisted functionality, Personal Data contained within Customer Content is processed only to provide the requested Services.

ServeusAI does not independently determine new purposes for processing Customer Content when acting as a Data Processor.

AI processing is performed under the same legal basis applicable to the Customer's use of the Services and is further governed by the applicable Data Processing Agreement.

Balancing Legitimate Interests

Where processing is based on legitimate interests, ServeusAI considers factors including:

- the reasonable expectations of individuals;
- the nature of the Personal Data;
- the necessity of the processing;
- the potential impact on individual rights;
- available safeguards; and
- the proportionality of the processing.

Where appropriate, additional technical and organizational measures are implemented to reduce privacy risks.

Changes to Processing Purposes

If ServeusAI intends to process Personal Data for a purpose that is materially different from the purpose for which it was originally collected, we will provide additional information where required by applicable law before commencing the new processing activity.

Summary

ServeusAI processes Personal Data only where an appropriate legal basis exists under applicable data protection laws.

Depending on the circumstances, processing is based on:

- performance of a contract;
- legitimate interests;
- compliance with legal obligations;
- consent;
- protection of vital interests; or
- other lawful grounds recognized under applicable law.

We regularly review our processing activities to ensure that the legal basis remains appropriate and that Personal Data continues to be processed fairly, transparently and responsibly.

8. AI Processing

Overview

Artificial Intelligence ("AI") is a core component of the Minerva platform and enables Customers to automate document analysis, information extraction and knowledge discovery.

This section explains how Personal Data may be processed when Customers choose to use AI-assisted functionality.

AI functionality is optional and is activated only in response to actions initiated by authorized Customer users.

AI Features

Minerva offers AI-assisted capabilities designed to improve productivity and accelerate document-centric workflows.

Depending on the functionality selected by the Customer, AI may be used to:

- analyze documents;
- extract structured information;
- summarize content;
- answer questions about uploaded documents;
- compare documents;
- classify information;
- identify relevant clauses;
- generate structured outputs; and
- support other document intelligence features.

Customers determine whether and how these features are used.

AI Service Providers

To provide AI-assisted functionality, ServeusAI integrates with selected third-party AI providers.

At the time of publication, these providers include:

- OpenAI; and
- Anthropic.

These providers process information solely to perform the requested inference operation.

Approved AI providers are identified in our Subprocessor List and are contractually engaged to support the delivery of the Services.

Information Processed by AI Providers

When AI functionality is used, the information transmitted to AI providers may include only the data necessary to complete the requested task.

Depending on the Customer's request, this may include:

- prompts;
- document text;
- extracted information;
- document fragments;
- metadata necessary for processing; and
- instructions generated by the Minerva platform.

The information transmitted depends on the feature selected by the Customer and the nature of the uploaded content.

Purpose of AI Processing

Personal Data is processed by AI providers solely for the purpose of providing the functionality requested by the Customer.

ServeusAI does not use AI providers to independently analyze Customer information for unrelated purposes.

AI processing is limited to supporting the operation of the Services and improving the Customer's requested workflow.

Customer Control

Customers remain responsible for deciding:

- which documents are uploaded;
- which users may access AI functionality;
- when AI-assisted processing is initiated;
- which AI-generated outputs are relied upon; and
- whether specific information is appropriate for AI processing.

Customers should ensure that their use of AI functionality complies with applicable legal, contractual and regulatory requirements.

AI Model Training

ServeusAI does **not** use Customer Content submitted through Minerva to train proprietary artificial intelligence models.

In particular, ServeusAI does not use Customer Content to:

- train foundation models;
- create commercial datasets;
- develop advertising profiles;
- build customer profiles; or
- improve proprietary AI models unrelated to providing the Services.

Customer Content remains under the control of the Customer, subject to the applicable contractual agreements.

Accuracy of AI Outputs

AI-generated responses are probabilistic in nature and may occasionally contain inaccuracies, omissions or incomplete information.

Customers remain responsible for reviewing and validating AI-generated outputs before relying upon them for:

- legal decisions;
- financial decisions;
- regulatory compliance;
- contractual matters;
- business-critical activities; or
- any other decision where accuracy is essential.

AI functionality is intended to support human decision-making rather than replace professional judgement.

International Data Transfers

The Minerva platform is primarily hosted within Microsoft Azure in the West Europe region.

However, when AI-assisted functionality is used, information submitted for inference may be processed by AI providers outside the European Economic Area (EEA), depending on the provider's infrastructure and the selected service.

Where such transfers occur, ServeusAI relies on appropriate safeguards in accordance with applicable data protection laws, including contractual commitments and, where applicable, the European Commission's Standard Contractual Clauses (SCCs).

Additional information regarding international transfers is available in the Data Processing Agreement.

AI Security

ServeusAI implements technical and organizational measures designed to protect information processed through AI functionality.

These measures include:

- encrypted communications;
- authenticated access;
- approved AI providers;
- supplier risk assessments;
- contractual safeguards;
- operational monitoring;
- access controls;
- secure API integrations; and
- continuous security reviews.

AI providers are periodically evaluated as part of ServeusAI's supplier management and information security programs.

Customer Responsibilities

Customers are responsible for ensuring that information submitted for AI processing is appropriate for their intended purposes.

Customers should:

- review applicable legal obligations;
- avoid submitting information where AI processing is prohibited;
- implement appropriate internal governance;
- review AI-generated outputs before use;
- manage user permissions appropriately; and
- ensure that their use of AI complies with applicable laws and contractual obligations.

ServeusAI cannot determine whether Customer-specific use cases satisfy industry-specific regulatory requirements.

Future AI Governance

Artificial intelligence technologies continue to evolve rapidly.

ServeusAI continuously monitors developments relating to:

- AI security;
- privacy;
- regulatory requirements;
- industry standards;
- supplier practices;
- technical safeguards; and
- emerging risks.

Our AI governance framework will continue to evolve to support responsible, secure and transparent use of artificial intelligence.

Summary

Artificial intelligence enables Minerva to provide powerful document intelligence capabilities while maintaining appropriate safeguards for Personal Data.

ServeusAI is committed to ensuring that AI functionality is implemented responsibly, transparently and securely. Customers retain control over how AI is used within their organization and remain responsible for determining whether particular information is appropriate for AI-assisted processing.

9. Cookies & Analytics

Overview

ServeusAI uses cookies and similar technologies to ensure the proper operation of its websites and Services, improve user experience, maintain security and better understand how visitors interact with our products.

Certain cookies are essential for the operation of our websites and Services, while others are used only with the user's consent where required by applicable law.

Cookie preferences are managed through the **Usercentrics Consent Management Platform (CMP)**.

Additional information regarding cookies is available in our separate Cookie Policy.

What Are Cookies?

Cookies are small text files stored on a user's device when visiting a website.

Cookies may be used to:

- recognize returning visitors;
- maintain authenticated sessions;
- remember user preferences;
- improve website functionality;
- measure website usage;
- enhance security;
- support analytics; and
- manage consent preferences.

Cookies may be either first-party cookies placed by ServeusAI or third-party cookies provided by trusted service providers.

Categories of Cookies

ServeusAI uses the following categories of cookies.

Strictly Necessary Cookies

These cookies are required for the operation of the website and the Minerva platform.

They support functions such as:

- user authentication;
- session management;
- security;
- load balancing;
- consent management; and
- fraud prevention.

Because these cookies are necessary for the operation of the Services, they cannot generally be disabled through the consent banner.

Preference Cookies

Preference Cookies remember information that improves the user experience by storing choices made by users.

They may be used to remember:

- language preferences;
- interface settings;
- accessibility preferences;
- consent settings; and
- other user-selected configuration options.

These cookies improve the usability of our Services but are not essential for their basic functionality.

Analytics Cookies

Subject to applicable consent requirements, analytics cookies help ServeusAI understand how visitors interact with our websites.

Analytics information is used to:

- measure website traffic;
- identify popular content;
- improve navigation;
- understand feature adoption;
- identify technical issues; and
- improve the overall user experience.

Analytics information is evaluated in aggregated form wherever reasonably practicable.

Marketing Cookies

At the time of publication of this Privacy Policy, ServeusAI does not use Marketing Cookies for behavioural advertising or cross-site advertising. Should this change in the future, users will be informed and, where required by applicable law, consent will be obtained before such cookies are activated.

Analytics Technologies

ServeusAI currently uses the following analytics technologies:

- Google Analytics;
- Google Tag Manager; and

- other analytics technologies introduced from time to time with appropriate notice where required.

Google Tag Manager is used solely to manage website tags and does not independently collect Personal Data.

Google Analytics helps us understand website usage patterns and improve the performance of our websites and Services.

Consent Management

ServeusAI uses **Usercentrics** to manage user consent for cookies and similar technologies.

Visitors may:

- accept all cookies;
- reject non-essential cookies;
- customize cookie preferences; and
- withdraw previously granted consent.

Consent records are maintained to demonstrate compliance with applicable privacy legislation.

Managing Cookie Preferences

Users may change their cookie preferences at any time by:

- reopening the cookie preference center;
- changing browser settings where applicable; or
- deleting previously stored cookies.

Disabling certain cookies may affect the functionality or usability of parts of the Services.

Do Not Track

Some web browsers support "Do Not Track" (DNT) signals.

Because there is currently no universally accepted standard governing DNT responses, ServeusAI does not currently respond differently to such browser signals.

Should industry standards evolve, this approach may be updated.

Future Technologies

ServeusAI may introduce additional analytics or user experience technologies as the platform evolves.

Where required by applicable law, users will be informed and appropriate consent will be obtained before new non-essential technologies are activated.

Summary

Cookies and similar technologies help ServeusAI operate secure, reliable and user-friendly Services.

Only Strictly Necessary Cookies are required for the operation of the Services. Preference Cookies, Analytics Cookies and any other non-essential technologies are used only where permitted by applicable law and, where required, based on the user's consent.

10. Sharing Personal Data

Overview

ServeusAI does not sell Personal Data.

Personal Data is shared only where necessary to provide the Services, comply with legal obligations, protect our legitimate interests or where instructed by the Customer.

All third-party service providers receiving Personal Data are subject to contractual, technical and organizational safeguards appropriate to the nature of the processing.

Service Providers

ServeusAI uses carefully selected third-party providers to support the operation of its business and the Minerva platform.

Depending on the Services used, Personal Data may be shared with providers including:

- Microsoft Azure (cloud hosting and infrastructure);

- OpenAI (AI inference services);
- Anthropic (AI inference services);
- Cloudflare (network security and content delivery);
- Google Workspace (business communications);
- Google Analytics (website analytics);
- Google Tag Manager (tag management);
- Usercentrics (cookie consent management);
- Vanta (security compliance and governance); and
- Namecheap (domain registration and DNS services).

These providers process Personal Data only for purposes consistent with the services they provide to ServeusAI.

Subprocessors

Where ServeusAI acts as a Data Processor on behalf of Customers, approved Subprocessors may process Customer Personal Data as necessary to deliver the Services.

ServeusAI maintains and periodically reviews its list of approved Subprocessors.

Customers may obtain the current Subprocessor List through the Trust Center or as part of the applicable Data Processing Agreement.

AI Providers

When Customers use AI-assisted functionality, relevant Customer Content may be transmitted to approved AI providers solely for the purpose of generating the requested response.

ServeusAI does not authorize AI providers to process Customer Content for purposes unrelated to providing the requested AI functionality.

Additional information regarding AI processing is provided in the Data Processing Agreement and Security Overview.

Within the ServeusAI Organization

Access to Personal Data within ServeusAI is limited to personnel who require access to perform their assigned responsibilities.

Examples include:

- engineering;

- customer support;
- security;
- compliance;
- finance;
- sales; and
- management.

Access is granted according to the principles of least privilege and need-to-know.

Legal Requirements

ServeusAI may disclose Personal Data where required by applicable law or where disclosure is reasonably necessary to:

- comply with legal obligations;
- respond to lawful requests from competent authorities;
- protect legal rights;
- investigate suspected unlawful activity;
- enforce contractual rights;
- protect the security of the Services; or
- protect the rights, safety or property of ServeusAI, its Customers or others.

Where legally permitted, we will seek to limit the scope of any disclosure.

Corporate Transactions

If ServeusAI becomes involved in a merger, acquisition, investment, reorganization or sale of assets, Personal Data may be transferred as part of that transaction.

Where appropriate, Personal Data will continue to be protected under obligations substantially consistent with this Privacy Policy.

Affected individuals will be informed where required by applicable law.

Professional Advisors

ServeusAI may disclose Personal Data to trusted professional advisors where necessary for legitimate business purposes.

These may include:

- legal advisors;

- accountants;
- auditors;
- insurance providers; and
- regulatory consultants.

Such disclosures are limited to information reasonably necessary for the relevant purpose.

No Sale of Personal Data

ServeusAI does not:

- sell Personal Data;
 - rent Personal Data;
 - trade Personal Data;
 - use Customer Content for advertising;
 - create advertising profiles based on Customer Content; or
 - disclose Personal Data for unrelated commercial purposes.
-

Summary

ServeusAI shares Personal Data only where necessary to provide the Services, comply with legal obligations or support legitimate business operations.

Third-party providers are carefully selected, contractually managed and periodically reviewed as part of our information security and supplier management programs.

11. International Data Transfers

Overview

ServeusAI primarily provides its Services from infrastructure located within the European Economic Area (EEA).

However, due to the global nature of cloud computing and artificial intelligence services, certain Personal Data may be transferred to or processed outside the EEA.

Where such transfers occur, ServeusAI implements appropriate safeguards in accordance with Chapter V of the GDPR.

Primary Hosting Location

The Minerva platform is primarily hosted within Microsoft Azure in the **West Europe** region.

Customer Content and production workloads are generally stored within Microsoft Azure infrastructure located in the European Economic Area.

AI Processing

When Customers use AI-assisted functionality, relevant Customer Content may be processed by approved AI providers.

Depending on the selected provider and available infrastructure, this processing may occur outside the European Economic Area.

Such transfers occur only to provide the AI functionality requested by the Customer.

Appropriate Safeguards

Where Personal Data is transferred internationally, ServeusAI relies on one or more appropriate safeguards, which may include:

- Standard Contractual Clauses (SCCs) approved by the European Commission;
 - contractual commitments with service providers;
 - adequacy decisions adopted by the European Commission;
 - supplementary technical and organizational measures; and
 - other lawful transfer mechanisms recognized under applicable law.
-

Assessment of Service Providers

Before engaging third-party providers that may process Personal Data internationally, ServeusAI considers factors including:

- security controls;
- privacy practices;
- contractual commitments;
- operational resilience;
- regulatory compliance;
- reputation; and
- overall supplier risk.

Supplier assessments form part of ServeusAI's ongoing vendor management program.

Customer Content

Where ServeusAI acts as a Data Processor, international transfers of Customer Content occur only as necessary to provide the Services and in accordance with the applicable Data Processing Agreement.

Customers remain responsible for determining whether such transfers are appropriate for their own regulatory obligations.

Future Changes

ServeusAI continuously monitors developments relating to international data transfers, including changes to applicable legislation, regulatory guidance and court decisions.

Where necessary, our contractual arrangements and operational practices will be updated to maintain compliance with applicable data protection laws.

Summary

ServeusAI is committed to ensuring that international transfers of Personal Data are conducted lawfully and securely.

Where Personal Data is transferred outside the European Economic Area, appropriate contractual and organizational safeguards are implemented to protect the rights and freedoms of individuals in accordance with the GDPR.

12. Data Retention

Overview

ServeusAI retains Personal Data only for as long as necessary to fulfil the purposes for which it was collected, to provide the Services, comply with legal obligations, resolve disputes and enforce contractual rights.

Retention periods vary depending on the category of information, the applicable contractual relationship and relevant legal or regulatory requirements.

Where Personal Data is no longer required, it is securely deleted or anonymized where appropriate.

Customer Content

Customer Content uploaded to the Minerva platform is retained for the duration of the Customer's subscription or other applicable contractual relationship.

Upon termination or expiration of the Agreement:

- the Customer may export its Customer Content during the applicable post-termination access period;
 - Customer Content is retained for up to **thirty (30) days** following termination to facilitate data export and account recovery where applicable; and
 - following the retention period, Customer Content is permanently deleted from production systems in accordance with documented deletion procedures, unless continued retention is required by applicable law.
-

Account Information

Information relating to user accounts is retained for as long as the account remains active.

Following account closure, certain account information may be retained where necessary to:

- comply with legal obligations;
- resolve disputes;
- enforce contractual rights;
- maintain audit records; or
- protect the security of the Services.

Information no longer required for these purposes is securely deleted or anonymized.

Operational Logs

Operational, security and application logs are retained for a limited period to support:

- platform security;
- incident investigations;
- troubleshooting;
- fraud prevention;
- operational monitoring; and
- compliance activities.

Unless a longer retention period is required for security, legal or regulatory purposes, operational logs are generally retained for approximately **ninety (90) days**.

Support Records

Customer support records, including support tickets and related communications, may be retained to:

- provide ongoing customer support;
- improve service quality;
- maintain support history;
- investigate recurring issues;
- comply with legal obligations; and
- establish or defend legal claims.

Support records are retained only for as long as reasonably necessary for these purposes.

Financial Records

ServeusAI retains accounting, invoicing and financial records for the periods required by applicable tax, accounting and commercial legislation.

These retention periods are determined by applicable legal requirements and may extend beyond the duration of the contractual relationship.

Marketing Information

Where Personal Data is processed for marketing purposes based on consent, the information will be retained until:

- consent is withdrawn;
- the individual unsubscribes;
- the information is no longer required; or
- applicable legal requirements require its deletion.

Withdrawal of consent does not affect processing that occurred prior to the withdrawal.

Backup Data

Backups are maintained to support business continuity and disaster recovery.

Backup copies are:

- encrypted;
- protected by appropriate access controls;
- retained in accordance with documented operational procedures; and
- automatically overwritten or securely deleted in accordance with backup lifecycle management.

Backup data is not maintained indefinitely.

Legal Hold

ServeusAI may retain Personal Data beyond normal retention periods where necessary to:

- comply with legal obligations;
- respond to regulatory investigations;
- preserve evidence;
- establish, exercise or defend legal claims; or
- comply with lawful instructions from competent authorities.

Where a legal hold applies, deletion may be delayed until the relevant obligation has been satisfied.

Secure Deletion

When Personal Data reaches the end of its retention period, ServeusAI applies appropriate deletion procedures.

Depending on the nature of the information, deletion may include:

- permanent deletion from production systems;
- deletion from active databases;
- removal from application storage;
- scheduled removal from backups where applicable; or
- anonymization where continued statistical use is appropriate.

Deletion procedures are designed to reduce the risk of unauthorized recovery.

Periodic Review

Retention periods are periodically reviewed to ensure they remain:

- appropriate for the purposes of processing;
- consistent with contractual commitments;
- aligned with legal obligations; and
- proportionate to operational requirements.

Where appropriate, retention schedules are updated as part of ServeusAI's information governance program.

Summary

ServeusAI retains Personal Data only for as long as necessary to provide the Services, fulfil contractual commitments and comply with applicable legal obligations.

Once Personal Data is no longer required, it is securely deleted or anonymized using documented operational procedures.

13. Your Rights

Overview

Individuals whose Personal Data is processed by ServeusAI may have certain rights under the General Data Protection Regulation (GDPR) and other applicable data protection laws.

The availability of these rights depends on the circumstances of the processing and whether ServeusAI is acting as a Data Controller or a Data Processor.

Where ServeusAI processes Personal Data solely on behalf of a Customer, requests relating to Customer Content should generally be directed to the relevant Customer acting as the Data Controller.

Right of Access

You may request confirmation as to whether ServeusAI processes your Personal Data.

Where applicable, you may also request access to:

- the Personal Data being processed;
- the purposes of processing;
- categories of Personal Data;

- recipients of the information;
 - applicable retention periods; and
 - other information required by applicable law.
-

Right to Rectification

You have the right to request that inaccurate or incomplete Personal Data be corrected.

ServeusAI will take reasonable steps to update inaccurate information where we are responsible for the processing.

Right to Erasure

In certain circumstances, you may request the deletion of your Personal Data.

This right may apply where:

- the information is no longer necessary;
- consent has been withdrawn;
- processing is unlawful;
- applicable law requires deletion; or
- another ground under Article 17 GDPR applies.

This right is subject to legal and contractual limitations.

Right to Restrict Processing

You may request that processing of your Personal Data be restricted in circumstances permitted under applicable law.

During a period of restriction, Personal Data may continue to be stored but will generally not be otherwise processed except where permitted by law.

Right to Data Portability

Where processing is based on consent or contract and carried out by automated means, you may request a copy of your Personal Data in a structured, commonly used and machine-readable format where required by applicable law.

Right to Object

You may object to certain processing activities based on legitimate interests.

Where a valid objection is received, ServeusAI will cease the relevant processing unless compelling legitimate grounds exist or the processing is otherwise permitted by law.

Right to Withdraw Consent

Where processing is based on consent, you may withdraw that consent at any time.

Withdrawal of consent does not affect the lawfulness of processing carried out before consent was withdrawn.

Right to Lodge a Complaint

If you believe that your Personal Data has been processed in violation of applicable data protection laws, you have the right to lodge a complaint with the competent supervisory authority.

Where possible, we encourage individuals to contact ServeusAI first so that we may seek to resolve concerns directly.

Exercising Your Rights

Requests relating to privacy rights may be submitted using the contact information provided in this Privacy Policy.

To protect Personal Data from unauthorized disclosure, ServeusAI may request additional information necessary to verify the identity of the individual submitting the request.

Requests will be handled within the timeframes required by applicable law.

Customer Content

Where Personal Data forms part of Customer Content uploaded to Minerva, ServeusAI generally acts solely as a Data Processor.

Accordingly, requests relating to:

- access;
- correction;
- deletion;
- restriction;
- portability; or
- objection

should normally be directed to the relevant Customer responsible for determining the purposes and means of processing.

ServeusAI will assist Customers in responding to such requests where required under the applicable Data Processing Agreement.

Summary

ServeusAI respects the privacy rights of individuals and is committed to supporting the exercise of those rights in accordance with applicable data protection legislation.

Where ServeusAI acts as a Data Controller, requests are handled directly. Where ServeusAI acts as a Data Processor, we assist our Customers in fulfilling their legal obligations.

14. Security

Overview

ServeusAI is committed to protecting Personal Data through appropriate technical and organizational measures designed to safeguard the confidentiality, integrity and availability of information.

Our security program is based on recognized industry practices and is continuously reviewed and improved as our products, technologies and regulatory obligations evolve.

Security Measures

ServeusAI implements security measures including, where appropriate:

- encryption of data in transit using TLS;
- encryption of data at rest using Microsoft Azure services;
- role-based access control (RBAC);

- least privilege access management;
- Multi-Factor Authentication for privileged accounts;
- security monitoring;
- operational logging;
- vulnerability management;
- backup and recovery procedures;
- supplier risk management; and
- documented incident response procedures.

These controls are intended to reduce the likelihood of unauthorized access, disclosure, alteration or destruction of Personal Data.

Organizational Security

Information security is supported through documented policies and operational procedures covering areas including:

- access management;
- acceptable use;
- supplier management;
- secure software development;
- incident response;
- business continuity;
- risk management;
- employee security awareness; and
- ongoing compliance activities.

Security responsibilities are assigned to appropriate personnel within the organization.

Continuous Improvement

ServeusAI continuously reviews its security controls through:

- internal assessments;
- risk reviews;
- supplier evaluations;
- vulnerability management;
- security monitoring;
- incident investigations; and
- ongoing compliance activities.

ServeusAI currently uses **Vanta** to support security governance, evidence collection and continuous compliance monitoring as part of its preparation for **ISO/IEC 27001 certification**.

At the time of publication of this Privacy Policy, the organization is actively preparing for certification and continues to enhance its Information Security Management System (ISMS).

Security Incidents

ServeusAI maintains documented procedures for identifying, investigating and responding to security incidents.

Where required by applicable law or contractual commitments, affected Customers will be notified of Security Incidents involving Personal Data without undue delay.

Additional information regarding our security practices is available in the **ServeusAI Security Overview**.

Summary

Protecting Personal Data is a fundamental component of ServeusAI's operations.

Through technical safeguards, organizational controls and continuous improvement of our security program, we seek to maintain an appropriate level of protection for the information entrusted to us.

15. Children's Privacy

Overview

The Services provided by ServeusAI, including the Minerva platform, are designed exclusively for business and professional use.

Our Services are not intended for use by children and are not directed toward individuals under the age of eighteen (18), or any higher minimum age required under applicable law.

ServeusAI does not knowingly collect Personal Data directly from children.

No Intentional Collection

ServeusAI does not intentionally:

- create accounts for children;

- market products or services to children;
- collect Personal Data directly from children;
- profile children;
- monitor children's online activities; or
- design Services specifically for use by minors.

Our websites, products and services are intended for organizations, businesses and professional users.

Customer Responsibility

Customers are responsible for ensuring that the information they upload to the Minerva platform complies with applicable laws and internal policies.

If Customer Content contains Personal Data relating to children, the Customer remains responsible for:

- establishing an appropriate legal basis for processing;
- obtaining any required permissions or consents;
- complying with applicable child protection legislation; and
- ensuring that such information is appropriate for processing within the Services.

ServeusAI processes such information solely on the documented instructions of the Customer when acting as a Data Processor.

If We Become Aware

If ServeusAI becomes aware that Personal Data has been collected directly from a child in circumstances where such collection was not intended or permitted, we will take reasonable steps to:

- investigate the matter;
 - restrict access where appropriate;
 - delete the information where legally permissible; and
 - take any additional action required under applicable law.
-

Summary

ServeusAI does not knowingly collect Personal Data directly from children and provides its Services exclusively for business and professional users.

16. Changes to this Privacy Policy

Overview

ServeusAI may update this Privacy Policy from time to time to reflect changes in:

- applicable laws;
- regulatory guidance;
- our products and services;
- security practices;
- business operations;
- technology;
- third-party service providers; or
- organizational structure.

We encourage users to review this Privacy Policy periodically to remain informed about how Personal Data is processed.

Notification of Changes

Where changes are material, ServeusAI may provide notice through one or more of the following methods:

- publication on our website;
- notification within the Minerva platform;
- email notification to registered Customers;
- updates through the Trust Center; or
- other appropriate communication channels.

The method of notification will depend on the nature and significance of the changes.

Effective Date

The "Effective Date" shown at the beginning of this Privacy Policy indicates when the current version became effective.

The "Last Updated" date reflects the most recent revision.

Continued use of the Services after an updated Privacy Policy becomes effective constitutes acknowledgment of the revised Policy, except where applicable law requires additional consent.

Previous Versions

ServeusAI may retain previous versions of this Privacy Policy for internal governance, audit and compliance purposes.

Historical versions may be made available upon reasonable request where appropriate.

Summary

Privacy requirements evolve over time.

ServeusAI is committed to maintaining an accurate, transparent and up-to-date Privacy Policy that reflects our current data protection practices.

17. Contact Information

Privacy Enquiries

Questions regarding this Privacy Policy or the processing of Personal Data may be directed to ServeusAI using the contact information published on our website.

Privacy-related enquiries may include:

- requests to exercise GDPR rights;
 - questions regarding Personal Data processing;
 - requests relating to Customer Content;
 - concerns regarding privacy or security;
 - questions concerning international data transfers; and
 - general privacy enquiries.
-

Customer Support

Customers requiring assistance with the Minerva platform should contact the ServeusAI support team using the support channels provided within the Services or through our website.

Support requests involving Customer Content may require verification of the requester's identity and authority.

Security Reporting

Individuals wishing to report suspected security vulnerabilities or security incidents are encouraged to use the security contact details published within the ServeusAI Trust Center.

ServeusAI investigates reported security issues in accordance with its documented Incident Response procedures and Responsible Disclosure Policy.

Supervisory Authorities

Individuals located within the European Economic Area have the right to lodge a complaint with the competent supervisory authority if they believe that the processing of their Personal Data infringes applicable data protection legislation.

Nothing in this Privacy Policy limits any statutory rights available under applicable law.

Additional Information

Additional information regarding ServeusAI's privacy and security practices is available through the ServeusAI Trust Center, including:

- Terms of Service;
- Data Processing Agreement (DPA);
- Security Overview;
- Cookie Policy;
- Approved Subprocessor List;
- Responsible Disclosure Policy; and
- other compliance documentation published from time to time.

Contact Details

The current contact information for ServeusAI is available on the official website.

Where dedicated contact addresses are established for privacy, security or compliance matters, this Privacy Policy and the Trust Center will be updated accordingly.

Final Statement

ServeusAI is committed to protecting the privacy, confidentiality and security of Personal Data entrusted to us by our Customers, users and business partners.

We believe that responsible data protection is an essential component of trustworthy AI services. Through transparent governance, strong technical and organizational safeguards, continuous security improvements and ongoing compliance efforts, we strive to ensure that Personal Data is processed lawfully, fairly and securely throughout its lifecycle.

As our Services and regulatory obligations continue to evolve, ServeusAI will continue to enhance its privacy program to maintain the trust placed in us by our Customers and stakeholders.