

DATA PROCESSING AGREEMENT

Effective Date: 6 July 2026

Version 2.0

This Data Processing Agreement ("**DPA**") forms part of the Agreement between **ServeusAI Kft.** ("**Processor**", "**ServeusAI**", "**we**", "**our**") and the customer identified in the applicable Agreement ("**Controller**" or "**Customer**").

This DPA governs the Processing of Personal Data by ServeusAI on behalf of the Customer in connection with the Services and is intended to satisfy the requirements of Article 28 of Regulation (EU) 2016/679 ("GDPR") and other Applicable Data Protection Laws.

1. Purpose and Scope

1.1 Purpose

The purpose of this DPA is to establish the rights and obligations of the Parties regarding the Processing of Customer Personal Data performed by ServeusAI while providing the Services.

This DPA sets out the contractual safeguards required under Applicable Data Protection Laws and forms an integral part of the Agreement.

1.2 Scope

This DPA applies whenever ServeusAI Processes Personal Data on behalf of the Customer in its capacity as a Processor.

The DPA governs all Processing activities performed in connection with the Services, including the collection, storage, organization, retrieval, use, transmission, analysis, deletion and other Processing operations necessary to provide and support the Services.

1.3 Precedence

To the extent of any conflict relating specifically to the Processing of Personal Data:

1. Applicable Data Protection Laws shall prevail;
2. this DPA shall prevail over the Agreement;
3. the Agreement shall prevail over any Order Form or Statement of Work.

This order of precedence applies solely to matters concerning the Processing of Personal Data.

1.4 Applicability

This DPA applies for the entire duration of the Agreement and remains effective for as long as ServeusAI Processes Customer Personal Data on behalf of the Customer.

Certain provisions relating to confidentiality, security, deletion, international transfers and liability shall survive termination of the Agreement to the extent required by Applicable Data Protection Laws.

2. Definitions

Unless otherwise defined in the Agreement, the following terms shall have the meanings set out below.

2.1 Applicable Data Protection Laws

"**Applicable Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under this DPA, including, where applicable:

- Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR);
 - the UK GDPR;
 - the UK Data Protection Act 2018;
 - the Swiss Federal Act on Data Protection (FADP);
 - and any legislation implementing, replacing or supplementing the foregoing.
-

2.2 Agreement

"Agreement" means the agreement governing the Customer's use of the Services, including any applicable Order Forms, Statements of Work and documents expressly incorporated by reference.

2.3 Customer Personal Data

"Customer Personal Data" means any Personal Data contained within Customer Content or otherwise Processed by ServeusAI on behalf of the Customer in connection with the Services.

Customer Personal Data does not include information Processed by ServeusAI as an independent Controller, where applicable.

2.4 Customer Content

"Customer Content" means all information, documents, files, prompts, instructions and other materials submitted to the Services by or on behalf of the Customer.

2.5 Controller

"Controller" has the meaning assigned under Applicable Data Protection Laws and refers to the Customer when determining the purposes and means of the Processing of Customer Personal Data.

2.6 Processor

"Processor" means ServeusAI acting on behalf of the Customer in accordance with this DPA and Applicable Data Protection Laws.

2.7 Personal Data

"Personal Data" means any information relating to an identified or identifiable natural person, as defined under Applicable Data Protection Laws.

2.8 Processing

"Processing" means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, transmission, alignment, restriction, erasure or destruction.

2.9 Services

"Services" means the software-as-a-service platform, related applications, APIs and associated support services provided by ServeusAI under the Agreement.

2.10 Subprocessor

"Subprocessor" means any third party engaged by ServeusAI to Process Customer Personal Data on behalf of the Customer.

2.11 Supervisory Authority

"Supervisory Authority" means an independent public authority established under Applicable Data Protection Laws with responsibility for monitoring compliance with those laws.

3. Roles of the Parties

3.1 Customer as Controller

Except where otherwise expressly agreed in writing, the Customer acts as the Controller of Customer Personal Data.

The Customer is solely responsible for:

- determining the purposes and legal basis for the Processing of Personal Data;
 - ensuring that Customer Personal Data has been lawfully collected;
 - providing all required privacy notices;
 - obtaining any required consents;
 - responding to Data Subject requests; and
 - complying with all obligations applicable to a Controller under Applicable Data Protection Laws.
-

3.2 ServeusAI as Processor

ServeusAI acts solely as a Processor and shall Process Customer Personal Data only on behalf of and in accordance with the documented instructions of the Customer, unless otherwise required by Applicable Data Protection Laws.

Where applicable law requires Processing beyond the Customer's instructions, ServeusAI shall inform the Customer before carrying out such Processing, unless prohibited by law.

3.3 Independent Controller Activities

Nothing in this DPA prevents ServeusAI from Processing Personal Data as an independent Controller where such Processing is required to:

- comply with legal obligations;
- establish, exercise or defend legal claims;
- maintain financial, accounting or tax records;
- ensure information security;
- prevent fraud or abuse of the Services; or
- comply with regulatory requirements applicable to ServeusAI.

Such Processing shall remain outside the scope of this DPA and shall be governed by ServeusAI's Privacy Policy or other applicable legal basis.

3.4 Customer Instructions

The Customer instructs ServeusAI to Process Customer Personal Data solely for the purpose of providing, securing, maintaining and supporting the Services in accordance with the Agreement and this DPA.

ServeusAI shall promptly inform the Customer if, in its opinion, an instruction infringes Applicable Data Protection Laws. Unless legally required to proceed, ServeusAI may suspend the relevant Processing until the Customer confirms or modifies the instruction.

4. Processing of Customer Personal Data

4.1 General Processing Obligation

ServeusAI shall Process Customer Personal Data solely on behalf of the Customer and only to the extent necessary to provide the Services in accordance with the Agreement, this DPA and the Customer's documented instructions.

ServeusAI shall not Process Customer Personal Data for its own purposes except where acting as an independent Controller under Section 3.3 or where required by Applicable Data Protection Laws.

4.2 Nature of the Processing

The nature, purpose, duration of the Processing, categories of Personal Data and categories of Data Subjects are described in **Annex I**.

The Parties acknowledge that the exact scope of Processing depends on the Services selected by the Customer and the Customer's use of those Services.

4.3 Customer Responsibility

The Customer is solely responsible for determining:

- whether Personal Data should be submitted to the Services;
 - the categories of Personal Data Processed;
 - the applicable legal basis for Processing;
 - compliance with transparency obligations;
 - compliance with sector-specific legal requirements; and
 - the accuracy and lawfulness of Customer Personal Data.
-

4.4 Compliance with Instructions

ServeusAI shall immediately notify the Customer if it reasonably believes that any documented instruction infringes Applicable Data Protection Laws.

Unless legally required to continue Processing, ServeusAI may suspend the affected Processing until the Customer confirms or modifies its instructions.

4.5 Prohibited Instructions

ServeusAI shall not be required to comply with any instruction that:

- violates Applicable Data Protection Laws;
- materially compromises the security of the Services;
- requires unlawful disclosure of Confidential Information;
- exceeds the scope of the Agreement; or
- would expose ServeusAI or its personnel to unlawful liability.

The Parties shall cooperate in good faith to identify a lawful alternative where reasonably practicable.

5. Confidentiality and Personnel

5.1 Confidentiality Commitment

ServeusAI shall ensure that all persons authorized to Process Customer Personal Data are subject to appropriate confidentiality obligations, whether contractual or statutory, and receive access only where necessary for the performance of their duties.

5.2 Need-to-Know Principle

Access to Customer Personal Data shall be granted solely to personnel who require such access for the provision, maintenance, security or support of the Services.

ServeusAI shall apply the principle of least privilege when assigning access rights.

5.3 Personnel Training

ServeusAI shall maintain an information security and privacy awareness program appropriate to the nature of the Services.

Personnel with access to Customer Personal Data shall receive periodic training regarding information security, confidentiality and applicable data protection obligations.

5.4 Personnel Responsibilities

Authorized personnel shall be required to:

- protect the confidentiality of Customer Personal Data;
 - comply with applicable security policies;
 - promptly report suspected security incidents; and
 - Process Customer Personal Data solely within the scope of their assigned responsibilities.
-

5.5 Termination of Access

ServeusAI shall maintain procedures designed to ensure that access to Customer Personal Data is removed or appropriately modified when personnel no longer require such access.

6. Technical and Organisational Measures

6.1 General Security Obligation

Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the Processing, and the risks to the rights and freedoms of natural persons, ServeusAI shall implement and maintain appropriate technical and organisational measures designed to protect Customer Personal Data.

6.2 Security Measures

ServeusAI maintains technical and organisational measures designed to provide an appropriate level of security, including measures relating to:

- access control;
- authentication;
- encryption;
- system security;
- network protection;
- vulnerability management;
- secure software development;
- monitoring and logging;
- backup and recovery;
- incident response;
- business continuity; and
- supplier security management.

A high-level description of these measures is set out in **Annex II**.

6.3 Continuous Improvement

ServeusAI periodically reviews its technical and organisational measures to ensure that they remain appropriate in light of:

- changes in technology;
- emerging threats;
- operational requirements;
- regulatory developments; and
- recognized industry practices.

ServeusAI may update its security measures from time to time, provided that such updates do not materially reduce the overall level of protection afforded to Customer Personal Data.

6.4 Security Documentation

ServeusAI may make additional information regarding its information security program available through its Trust Center or other appropriate documentation.

Nothing in this DPA requires ServeusAI to disclose information that would:

- compromise the security of the Services;
- reveal trade secrets;
- disclose confidential internal procedures; or
- create an unreasonable security risk.

7. Subprocessors

7.1 General Authorization

The Customer hereby provides a general authorization for ServeusAI to engage Subprocessors for the Processing of Customer Personal Data, provided that ServeusAI complies with the requirements of this Section.

A current list of approved Subprocessors is maintained in **Annex III** or otherwise made available to the Customer through an appropriate notification mechanism.

7.2 Appointment of Subprocessors

ServeusAI shall conduct appropriate due diligence before engaging a Subprocessor and shall ensure that each Subprocessor is contractually bound to implement data protection obligations that are no less protective than those set out in this DPA, to the extent applicable to the services performed.

7.3 Changes to Subprocessors

ServeusAI may add or replace Subprocessors from time to time to support the operation, maintenance or improvement of the Services.

Where required by Applicable Data Protection Laws or agreed in the Agreement, ServeusAI shall provide advance notice of material changes to its Subprocessors.

7.4 Customer Objections

Where the Customer reasonably believes that a newly appointed Subprocessor is unable to provide adequate safeguards required under Applicable Data Protection Laws, the Customer may submit a written objection within thirty (30) days after receiving notice.

The Parties shall cooperate in good faith to identify a commercially reasonable solution. Where no reasonable solution can be reached, either Party may terminate only the affected Services in accordance with the Agreement.

7.5 Responsibility for Subprocessors

ServeusAI shall remain responsible for the performance of its Subprocessors to the extent required by Applicable Data Protection Laws.

The engagement of a Subprocessor shall not reduce ServeusAI's obligations under this DPA.

8. International Data Transfers

8.1 General Principle

ServeusAI shall not transfer Customer Personal Data outside the European Economic Area, the United Kingdom or Switzerland unless such transfer is carried out in accordance with Applicable Data Protection Laws.

8.2 Appropriate Safeguards

Where an international transfer requires additional safeguards, ServeusAI shall implement one or more legally recognized transfer mechanisms, including where appropriate:

- Standard Contractual Clauses approved by the European Commission;
 - the UK International Data Transfer Addendum;
 - adequacy decisions;
 - or any other legally recognized transfer mechanism available under Applicable Data Protection Laws.
-

8.3 Transfer Impact Assessments

Where required by Applicable Data Protection Laws, ServeusAI shall take reasonable measures to assess the legal and practical circumstances of international transfers and implement supplementary safeguards where appropriate.

8.4 Government Access Requests

Where legally permitted, ServeusAI shall promptly notify the Customer of any legally binding request from a public authority seeking access to Customer Personal Data.

Where appropriate, ServeusAI shall make commercially reasonable efforts to challenge requests that appear unlawful or disproportionate before disclosing Customer Personal Data.

9. Assistance to the Customer

9.1 General Assistance

Taking into account the nature of the Processing and the information available to ServeusAI, ServeusAI shall provide reasonable assistance to the Customer in fulfilling its obligations under Applicable Data Protection Laws.

9.2 Data Subject Requests

If ServeusAI receives a request directly from a Data Subject relating to Customer Personal Data, ServeusAI shall:

- promptly notify the Customer;
- refrain from responding directly unless legally required or expressly authorized by the Customer; and
- provide reasonable assistance to enable the Customer to respond.

The Customer remains responsible for responding to Data Subject requests.

9.3 Data Protection Impact Assessments

Where reasonably requested, ServeusAI shall provide information available to it that is necessary to assist the Customer in conducting:

- Data Protection Impact Assessments (DPIAs); and
- prior consultations with competent Supervisory Authorities,

to the extent required by Applicable Data Protection Laws.

9.4 Security Information

Upon reasonable request, ServeusAI shall make available information necessary to demonstrate compliance with its obligations under this DPA, provided that such disclosure:

- is proportionate;
 - does not compromise the security of the Services;
 - does not disclose confidential information of other customers; and
 - is subject to appropriate confidentiality obligations where necessary.
-

10. Personal Data Breaches

10.1 Notification Obligation

ServeusAI shall notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data.

Such notification shall be made as soon as reasonably practicable and, where feasible, sufficiently in advance to enable the Customer to comply with its own legal obligations.

10.2 Information Included in the Notification

To the extent reasonably available at the time of notification, ServeusAI shall provide information concerning:

- the nature of the Personal Data Breach;

- the categories of affected Personal Data;
- the likely consequences of the incident;
- measures taken or proposed to address the incident; and
- contact details for obtaining additional information.

Where all relevant information is not immediately available, ServeusAI may provide additional information in phases as the investigation progresses.

10.3 Investigation and Mitigation

ServeusAI shall take appropriate measures to:

- investigate the incident;
- mitigate adverse effects where reasonably possible;
- restore the security of the affected systems; and
- prevent recurrence where appropriate.

Nothing in this Section shall require ServeusAI to disclose information protected by legal privilege, confidential security procedures or information that would materially increase security risks.

10.4 No Admission of Liability

Notification of a Personal Data Breach under this Section shall not constitute an admission of fault, liability or legal responsibility by either Party.

11. Audit and Compliance

11.1 Demonstration of Compliance

Upon reasonable written request, ServeusAI shall make available to the Customer information necessary to demonstrate compliance with this DPA and Applicable Data Protection Laws.

Such information may include security documentation, policies, audit reports, certifications, compliance attestations, Subprocessor information and other materials reasonably available to ServeusAI.

11.2 Customer Audits

Where required by Applicable Data Protection Laws, the Customer may request an audit of ServeusAI's Processing activities relevant to this DPA.

Before requesting an on-site audit, the Customer shall first review documentation made available by ServeusAI, including information available through ServeusAI's Trust Center or equivalent compliance materials.

If the available documentation reasonably demonstrates compliance, the Parties agree that no further audit activity shall ordinarily be required.

11.3 On-Site Audits

Where an on-site audit is required and cannot reasonably be satisfied through available documentation, the Parties shall cooperate in good faith to arrange an appropriate audit.

Any such audit shall:

- be conducted during normal business hours;
- be subject to reasonable advance written notice;
- avoid unnecessary disruption to ServeusAI's business operations;
- be limited to matters directly relevant to this DPA;
- be subject to appropriate confidentiality obligations; and
- comply with ServeusAI's security requirements.

ServeusAI may require that the auditor be independent and not a competitor of ServeusAI.

11.4 Audit Costs

Unless otherwise required by Applicable Data Protection Laws:

- the Customer shall bear its own audit costs;
 - the Customer shall reimburse ServeusAI for reasonable internal costs incurred in supporting extensive audit activities beyond normal compliance requests; and
 - no fee shall apply for routine documentation made available through the Trust Center or standard compliance responses.
-

12. Return and Deletion of Customer Personal Data

12.1 Customer Ownership

As between the Parties, the Customer retains all rights, title and interest in and to Customer Content, including Customer Personal Data.

Nothing in this DPA transfers ownership of Customer Personal Data to ServeusAI.

12.2 Return of Customer Data

Upon termination or expiration of the Agreement, the Customer may request the return or export of Customer Content in accordance with the procedures described in the Agreement.

Where technically feasible, ServeusAI shall make Customer Content available for export using standard functionality provided by the Services.

12.3 Retention Following Termination

Unless otherwise agreed in writing, Customer Content shall remain available for retrieval for thirty (30) calendar days following termination or expiration of the Agreement.

Following expiration of the retrieval period, Customer Content shall become eligible for deletion in accordance with ServeusAI's internal retention procedures.

12.4 Deletion of Customer Personal Data

Following the applicable retention period, ServeusAI shall delete or render inaccessible Customer Personal Data within a commercially reasonable period, unless continued retention is required by:

- applicable law;
- a legally binding order of a competent authority;
- ongoing legal proceedings;
- legitimate information security requirements relating to backup media; or

- another lawful basis under Applicable Data Protection Laws.

Deletion activities may occur through automated operational processes.

12.5 Backup Copies

The Customer acknowledges that Customer Personal Data may continue to exist within encrypted backup media for a limited period following operational deletion.

Such backup copies shall be retained solely for disaster recovery and business continuity purposes and shall not be actively processed for business purposes except where restoration is operationally necessary.

12.6 Certification of Deletion

Upon reasonable written request, ServeusAI may confirm that Customer Personal Data has been deleted in accordance with this Section, except where deletion cannot be completed due to a legal retention obligation or another exception described above.

13. Liability

13.1 Application of Liability Provisions

This DPA forms an integral part of the Agreement.

Except as expressly provided in this DPA or where prohibited by Applicable Data Protection Laws, the liability of each Party arising out of or relating to this DPA shall be governed by the limitation of liability provisions contained in the Agreement.

13.2 Responsibility for Compliance

Each Party shall remain responsible for complying with the obligations imposed upon it under Applicable Data Protection Laws.

Nothing in this DPA shall relieve either Party of responsibilities assigned directly to it by applicable legislation.

13.3 Customer Responsibility

The Customer remains solely responsible for:

- determining the legal basis for Processing;
- complying with transparency obligations;
- obtaining any required consents;
- ensuring the lawful collection of Personal Data;
- determining which Personal Data is submitted to the Services;
- ensuring that Customer Content may lawfully be Processed using the Services; and
- complying with sector-specific legal or regulatory requirements applicable to the Customer.

ServeusAI shall not be responsible for unlawful or unauthorized Customer instructions or Customer Content.

13.4 Service Provider Responsibility

ServeusAI shall remain responsible for implementing and maintaining appropriate technical and organizational measures designed to protect Customer Personal Data in accordance with this DPA and Applicable Data Protection Laws.

ServeusAI shall use commercially reasonable efforts to maintain the security, confidentiality and availability of the Services.

13.5 Subprocessors

ServeusAI remains responsible for the performance of its approved Subprocessors as required under Applicable Data Protection Laws.

The appointment of a Subprocessor shall not reduce ServeusAI's obligations under this DPA.

13.6 No Indirect Damages

To the maximum extent permitted by applicable law, neither Party shall be liable under this DPA for any indirect, incidental, consequential, special, exemplary or punitive damages, including loss of profits, revenue, goodwill or business opportunities, except where such limitation is prohibited by Applicable Data Protection Laws.

14. Miscellaneous

14.1 Entire Agreement

This DPA forms an integral part of the Agreement between the Parties.

Together with the Agreement, any applicable Order Forms, Statements of Work and referenced policies, this DPA constitutes the entire agreement between the Parties relating to the Processing of Customer Personal Data.

14.2 Amendments

ServeusAI may amend this DPA from time to time where reasonably necessary to:

- comply with Applicable Data Protection Laws;
- reflect changes to the Services;
- implement new security measures;
- accommodate changes to Subprocessors;
- address regulatory guidance; or
- improve clarity and consistency.

Where a material amendment adversely affects the Customer's rights or obligations under this DPA, ServeusAI shall provide reasonable notice in accordance with the Agreement.

14.3 Governing Law and Jurisdiction

This DPA shall be governed by and interpreted in accordance with the governing law specified in the Agreement, unless otherwise required by mandatory provisions of Applicable Data Protection Laws.

Any dispute arising out of or relating to this DPA shall be subject to the jurisdiction specified in the Agreement, except where Applicable Data Protection Laws grant jurisdiction to another competent court or supervisory authority.

14.4 Severability

If any provision of this DPA is determined by a court or competent authority to be invalid, illegal or unenforceable, the remaining provisions shall remain in full force and effect.

The Parties shall cooperate in good faith to replace any invalid provision with a lawful provision that most closely reflects the original commercial and legal intent.

14.5 Survival

The provisions of this DPA relating to confidentiality, security, international transfers, deletion obligations, liability, dispute resolution and any provisions which by their nature are intended to survive termination shall remain effective following termination or expiration of the Agreement.

ANNEX I

DETAILS OF PROCESSING ACTIVITIES

This Annex forms an integral part of the Data Processing Agreement and describes the Processing activities carried out by ServeusAI on behalf of the Customer in accordance with Article 28(3) GDPR.

A. Subject Matter of the Processing

ServeusAI provides the **Minerva** Software-as-a-Service platform, an AI-powered document intelligence solution that enables Customers to securely upload, organize, search, analyze and process documents and other Customer Content.

Processing is limited to the activities necessary to provide, maintain, secure and support the Services in accordance with the Agreement and the Customer's documented instructions.

B. Duration of the Processing

Processing shall continue for the duration of the Agreement.

Following termination or expiration of the Agreement, Customer Personal Data shall be retained only for the periods described in the Agreement and the DPA, after which it shall be deleted or rendered inaccessible unless continued retention is required by Applicable Data Protection Laws.

Where supported by the Services, Customer Content shall remain available for export during the post-termination retrieval period described in the Agreement.

C. Nature of the Processing

Depending on the Customer's use of the Services, Processing may include:

- collection;
 - upload;
 - storage;
 - hosting;
 - organization;
 - indexing;
 - retrieval;
 - viewing;
 - search;
 - artificial intelligence-assisted analysis;
 - extraction of structured information;
 - validation workflows;
 - export;
 - transmission;
 - backup;
 - deletion; and
 - customer support activities authorized by the Customer.
-

D. Purpose of the Processing

Customer Personal Data is Processed solely for purposes necessary to provide the Services, including:

- providing the Services;
- storing Customer Content;
- AI-assisted document processing;
- document search and retrieval;
- information extraction;
- maintaining service availability;
- information security;
- fraud prevention;
- customer support;
- business continuity;
- disaster recovery; and
- compliance with applicable legal obligations.

ServeusAI does **not** Process Customer Personal Data:

- for advertising purposes;
- for profiling individuals for marketing purposes; or

- to train proprietary foundation or general-purpose artificial intelligence models unless the Customer has expressly opted in through a separate written agreement.
-

E. Categories of Data Subjects

Depending upon the Customer's use of the Services, Customer Personal Data may relate to:

- employees;
- contractors;
- consultants;
- customers;
- prospective customers;
- suppliers;
- vendors;
- business partners;
- applicants;
- authorized representatives;
- end users;
- individuals identified within Customer documents; and
- other natural persons whose Personal Data the Customer chooses to submit to the Services.

The Customer determines which categories of Data Subjects are included within Customer Content.

F. Categories of Personal Data

Customer Personal Data may include any categories of Personal Data submitted by the Customer through the Services.

Depending upon Customer use, such information may include:

Identity Information

- name
- job title
- employee identifiers
- government-issued identifiers contained within Customer documents

Contact Information

- email address
- telephone number
- postal address
- business contact details

Employment Information

- employer
- department
- position
- organizational information

Financial and Commercial Information

- invoices
- contracts
- purchase orders
- quotations
- payment references
- tax-related information

Technical Information

- IP addresses
- user identifiers
- authentication events
- audit records
- device information
- browser metadata

Customer Documents

Any documents uploaded by the Customer using the Services, including text documents, spreadsheets, presentations, scanned documents, contracts, certificates, reports, images and other supported file formats.

AI Processing Inputs and Outputs

Where AI-assisted functionality is used, Processing may include prompts, extracted text, metadata, processing instructions and generated outputs.

G. Special Categories of Personal Data

The Services are not specifically designed for the routine Processing of Special Categories of Personal Data as defined under Article 9 GDPR.

Where the Customer chooses to upload documents containing Special Categories of Personal Data, the Customer remains solely responsible for:

- determining the legal basis for such Processing;
- complying with transparency obligations;
- implementing any additional safeguards required by law; and
- ensuring compliance with Applicable Data Protection Laws.

ServeusAI shall Process such information solely in accordance with the Customer's documented instructions.

H. Frequency of Processing

Processing occurs on a continuous basis for the duration of the Customer's use of the Services and is initiated solely through Customer activity or automated operations necessary to provide, secure and maintain the Services.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

Version 1.0

Effective Date: [Effective Date]

This document forms **Annex II** to the Data Processing Agreement ("DPA") between **ServeusAI Kft.** ("ServeusAI") and the Customer.

These Technical and Organisational Measures ("TOMs") describe the security controls implemented by ServeusAI to protect Customer Personal Data processed through the Minerva platform.

The measures described herein are designed to satisfy the requirements of Article 32 of the GDPR and other Applicable Data Protection Laws.

1. Purpose and Scope

1.1 Purpose

The purpose of this document is to describe the technical and organisational measures implemented by ServeusAI to ensure an appropriate level of security for Customer Personal Data.

These measures are intended to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, unauthorized access and other forms of unlawful Processing.

1.2 Scope

These measures apply to all systems, personnel, contractors and subprocessors involved in the Processing of Customer Personal Data as part of the Services.

The controls described in this document apply throughout the lifecycle of Customer Personal Data, including collection, storage, use, transmission, backup and deletion.

1.3 Security Objectives

ServeusAI maintains an information security program designed to support the following objectives:

- confidentiality of Customer Personal Data;
 - integrity of systems and information;
 - availability and resilience of the Services;
 - protection against unauthorized access;
 - timely detection and response to security events;
 - continuous improvement of security controls; and
 - compliance with applicable legal and contractual obligations.
-

1.4 Risk-Based Approach

Technical and organisational measures are selected and maintained using a risk-based approach that considers:

- the nature of the Processing;
- the categories of Personal Data processed;
- the likelihood and severity of risks to individuals;
- the current state of technology;
- implementation costs; and
- evolving security threats.

Security controls are reviewed periodically and updated where necessary to maintain an appropriate level of protection.

2. Information Security Governance

2.1 Information Security Program

ServeusAI maintains an information security program designed to establish, implement, maintain and continuously improve the protection of Customer Personal Data and supporting information systems.

The program includes documented policies, defined responsibilities, risk management activities and security oversight appropriate to the size and complexity of the organization.

2.2 Security Policies

ServeusAI maintains and periodically reviews internal security policies and procedures covering areas including:

- information security;
- access management;
- acceptable use;
- incident response;
- business continuity;
- vulnerability management;
- secure software development; and
- supplier management.

Policies are reviewed and updated as necessary to reflect changes in legal requirements, technology and business operations.

2.3 Roles and Responsibilities

Information security responsibilities are assigned to appropriate personnel.

Individuals with security responsibilities are expected to:

- understand applicable security obligations;
 - protect confidential information;
 - report security incidents;
 - follow approved security procedures; and
 - participate in periodic security awareness activities.
-

2.4 Risk Management

ServeusAI periodically evaluates information security risks affecting the Services.

Risk assessments are used to identify potential threats, evaluate the effectiveness of existing controls and prioritize remediation activities where appropriate.

2.5 Continuous Improvement

The information security program is reviewed on an ongoing basis to reflect:

- technological developments;
- emerging threats;
- changes in applicable legal requirements;
- customer expectations; and
- lessons learned from operational experience.

Where appropriate, security controls are enhanced to improve the overall security posture of the Services.

3. Identity and Access Management

3.1 Access Control Principles

Access to Customer Personal Data and production systems is granted only where required for legitimate business purposes.

Access permissions are assigned according to the principles of:

- least privilege;
 - need-to-know;
 - role-based access; and
 - segregation of responsibilities where appropriate.
-

3.2 Identity Management

ServeusAI maintains processes for provisioning, modifying and revoking user access throughout the identity lifecycle.

Access rights are reviewed periodically and adjusted when personnel responsibilities change or access is no longer required.

3.3 Authentication

Access to systems containing Customer Personal Data requires authentication using appropriate authentication mechanisms.

Where appropriate, multi-factor authentication is implemented for administrative or privileged access.

Authentication credentials are protected against unauthorized disclosure and misuse.

3.4 Privileged Access

Administrative privileges are restricted to authorized personnel whose responsibilities require elevated access.

Privileged activities are subject to additional monitoring and appropriate security controls designed to reduce the risk of unauthorized or accidental changes.

3.5 Access Revocation

Access permissions are removed or modified promptly following termination of employment, changes in responsibilities or other circumstances requiring access modification.

ServeusAI maintains procedures designed to ensure timely deprovisioning of user accounts.

4. Human Resource Security

4.1 Personnel Security

ServeusAI implements personnel security measures designed to ensure that individuals with access to Customer Personal Data understand and fulfil their information security and confidentiality responsibilities.

Personnel are granted access to Customer Personal Data only where such access is necessary for the performance of their assigned duties.

4.2 Confidentiality Obligations

Employees, contractors and other authorized personnel with access to Customer Personal Data are subject to appropriate confidentiality obligations.

Such obligations continue after the termination of employment or contractual engagement where required by applicable law or contractual commitments.

4.3 Security Awareness and Training

ServeusAI maintains an information security awareness program designed to promote secure handling of information and compliance with applicable security policies.

Personnel receive appropriate security and privacy training upon joining the organization and periodically thereafter.

Training is reviewed and updated to reflect changes in technology, emerging threats and regulatory requirements.

4.4 Acceptable Use

Personnel are expected to use information systems, communication tools and corporate assets in accordance with documented acceptable use requirements.

These requirements are intended to reduce information security risks and support the protection of Customer Personal Data.

4.5 Joiner, Mover and Leaver Process

ServeusAI maintains procedures governing the assignment, modification and removal of access rights throughout the personnel lifecycle.

These procedures are designed to ensure that:

- access rights are assigned based on business need;

- access is reviewed when responsibilities change;
 - privileged access is adjusted where appropriate; and
 - access is removed promptly when employment or contractual relationships end.
-

4.6 Disciplinary Process

Violations of information security policies or confidentiality obligations may be addressed through appropriate disciplinary or contractual measures, taking into account the nature and severity of the violation and applicable legal requirements.

5. Cryptographic Controls

5.1 Encryption Strategy

ServeusAI implements cryptographic controls designed to protect the confidentiality and integrity of Customer Personal Data during transmission, storage and processing, where appropriate.

The selection and use of cryptographic mechanisms are based on recognized industry practices and are periodically reviewed to ensure continued effectiveness.

5.2 Data in Transit

Customer Personal Data transmitted over public or untrusted networks is protected using secure communication protocols and encryption mechanisms designed to prevent unauthorized interception or modification.

Cryptographic protocols and configurations are reviewed periodically to maintain compatibility with current security standards.

5.3 Data at Rest

Customer Personal Data stored within the Services is protected using encryption mechanisms appropriate to the sensitivity of the data and the underlying storage technologies.

Encryption controls are intended to reduce the risk of unauthorized access to stored information.

5.4 Cryptographic Key Management

Cryptographic keys are managed throughout their lifecycle using processes designed to support their confidentiality, integrity and availability.

Access to cryptographic material is restricted to authorized processes or personnel where required, and key management practices are periodically reviewed.

5.5 Certificate Management

Digital certificates used to support secure communications are managed through documented processes covering issuance, renewal, replacement and revocation, where applicable.

ServeusAI monitors certificate validity and implements reasonable measures to reduce the risk of service disruption caused by expired or invalid certificates.

6. Operations Security

6.1 Operational Management

ServeusAI maintains operational procedures designed to support the secure, reliable and consistent delivery of the Services.

Operational activities are performed in accordance with documented processes intended to maintain the confidentiality, integrity and availability of Customer Personal Data.

6.2 Configuration Management

Systems supporting the Services are configured using standardized practices designed to promote security, consistency and operational stability.

Configuration changes are subject to appropriate review and control processes to reduce the risk of unintended security impacts.

6.3 Change Management

Changes affecting production environments are managed through controlled change management procedures.

Depending on the nature and risk of the change, activities may include planning, technical review, testing, approval, deployment verification and, where appropriate, rollback planning.

Emergency changes are subject to expedited procedures and are reviewed following implementation.

6.4 Vulnerability Management

ServeusAI maintains a vulnerability management process designed to identify, assess, prioritize and remediate security vulnerabilities affecting the Services.

Vulnerabilities are evaluated based on their potential impact and addressed within timeframes appropriate to the associated risk.

Where appropriate, vulnerability assessments, automated scanning and security testing are performed to support the effectiveness of the vulnerability management process.

6.5 Malware Protection

Appropriate preventive and detective measures are implemented to reduce the risk of malicious software affecting systems supporting the Services.

Security controls are periodically reviewed and updated to address evolving threats and changes in the operational environment.

6.6 Logging

Security-relevant events are recorded where appropriate to support operational monitoring, incident investigation, troubleshooting and compliance activities.

Access to logs is restricted to authorized personnel and appropriate measures are implemented to help preserve the integrity of logged information.

6.7 Monitoring

ServeusAI performs monitoring activities designed to identify operational anomalies, potential security events and conditions that may affect the availability or security of the Services.

Monitoring capabilities support the timely detection, investigation and response to security-related events.

6.8 Backup

Backup procedures are implemented to support the availability and recovery of Customer Personal Data and critical service components.

Backup activities are performed in accordance with documented procedures and are periodically reviewed to help ensure their continued effectiveness.

6.9 Recovery

Recovery procedures are maintained to support the restoration of service availability and Customer Personal Data following operational disruptions or other significant events.

Recovery capabilities are periodically evaluated and updated where appropriate to reflect changes in business requirements and the operational environment.

7. Physical and Environmental Security

7.1 Physical Security

ServeusAI delivers the Services using professionally managed cloud infrastructure operated by established cloud service providers.

Physical and environmental security controls relating to facilities, including physical access protection, environmental safeguards, power redundancy and facility monitoring, are implemented and maintained by the underlying cloud infrastructure provider.

ServeusAI is responsible for the security of the applications, customer data, identities and configurations within its operational control.

7.2 Asset Management

Information assets supporting the Services are identified and managed throughout their lifecycle.

Assets are assigned an appropriate level of protection based on their intended use, business importance and associated information security risks.

7.3 Media Handling and Disposal

Where Customer Personal Data is removed from operational systems, appropriate measures are implemented to prevent unauthorized disclosure.

Logical deletion processes are applied to cloud-hosted data, while physical storage media are managed and disposed of by the underlying infrastructure provider in accordance with applicable security standards.

8. Secure Development

8.1 Secure Development Lifecycle

ServeusAI integrates information security considerations throughout the software development lifecycle.

Security activities are incorporated into planning, implementation, testing, deployment and maintenance processes to reduce security risks and improve software quality.

8.2 Secure Coding Practices

Software is developed in accordance with secure coding principles intended to reduce common software vulnerabilities and improve application resilience.

Developers are expected to follow documented development standards and security requirements appropriate to their responsibilities.

8.3 Code Review

Changes affecting production software are reviewed before deployment through peer review or equivalent quality assurance activities.

Reviews are intended to identify implementation errors, security weaknesses and deviations from established development practices.

8.4 Security Testing

Security testing is incorporated into the development and deployment process as appropriate.

Testing activities may include automated analysis, dependency validation, vulnerability assessments and other verification activities designed to identify security weaknesses before deployment.

8.5 Software Dependencies

Third-party software components are evaluated as part of the software development process.

ServeusAI monitors software dependencies for publicly disclosed security vulnerabilities and takes appropriate remediation measures based on the assessed level of risk.

8.6 Change Deployment

Software releases are deployed using controlled operational procedures intended to minimize service disruption and reduce implementation risk.

Where appropriate, deployment activities include validation, monitoring and rollback capabilities.

9. Supplier Security

9.1 Supplier Selection

ServeusAI evaluates suppliers that may have access to Customer Personal Data or support critical service operations.

Supplier selection considers factors including security capabilities, operational reliability, legal compliance and contractual commitments.

9.2 Contractual Safeguards

Suppliers Processing Customer Personal Data on behalf of ServeusAI are required to enter into contractual arrangements imposing appropriate confidentiality, security and data protection obligations.

Where applicable, such obligations include the implementation of appropriate technical and organisational measures consistent with applicable data protection laws.

9.3 Supplier Monitoring

ServeusAI periodically reviews suppliers whose services may affect the security or availability of the Services.

The frequency and scope of such reviews are determined based on the supplier's role, the services provided and the associated level of risk.

9.4 Subprocessors

Subprocessors Processing Customer Personal Data are appointed in accordance with the Data Processing Agreement.

ServeusAI remains responsible for ensuring that Subprocessors are subject to appropriate contractual safeguards and that their engagement does not reduce the level of protection provided under the DPA.

10. Information Security Incident Management

10.1 Incident Management Framework

ServeusAI maintains documented procedures for identifying, reporting, assessing, responding to and resolving information security incidents.

These procedures are designed to support timely response while minimizing potential impacts on Customer Personal Data and the availability of the Services.

10.2 Incident Detection and Reporting

Personnel are expected to promptly report suspected or confirmed information security incidents through established internal reporting channels.

Reported incidents are assessed to determine their nature, potential impact and appropriate response.

10.3 Investigation and Response

Information security incidents are investigated using procedures appropriate to their severity and potential impact.

Response activities may include containment, eradication, recovery and the implementation of corrective actions designed to reduce the likelihood of recurrence.

10.4 Customer Notification

Where an incident constitutes a Personal Data Breach requiring notification under applicable data protection laws or contractual obligations, ServeusAI shall notify affected Customers without undue delay in accordance with the Data Processing Agreement.

10.5 Lessons Learned

Following significant information security incidents, ServeusAI evaluates the effectiveness of the response and identifies opportunities to strengthen security controls, operational procedures and personnel awareness.

11. Business Continuity

11.1 Business Continuity Planning

ServeusAI maintains business continuity arrangements designed to support the continued delivery of the Services during disruptive events.

Business continuity planning is intended to reduce operational disruption and support the timely restoration of critical services.

11.2 Disaster Recovery

Disaster recovery procedures are maintained to support the recovery of systems and Customer Personal Data following significant operational incidents.

Recovery capabilities are periodically reviewed and updated to reflect changes in the operational environment.

11.3 Resilience

ServeusAI designs and operates the Services with consideration for operational resilience and service availability.

Resilience measures are intended to reduce the impact of infrastructure failures, software defects and other operational disruptions.

12. Compliance and Continuous Improvement

12.1 Legal and Regulatory Compliance

ServeusAI maintains processes designed to support compliance with applicable legal, regulatory and contractual requirements relating to information security and the Processing of Customer Personal Data.

12.2 Internal Review

Information security measures are periodically reviewed to assess their continued suitability and effectiveness.

Reviews may consider changes in technology, business operations, legal requirements and the evolving threat landscape.

12.3 Risk Assessment

ServeusAI periodically assesses information security risks affecting the Services.

Assessment results are used to prioritize security improvements and support the ongoing development of the information security program.

12.4 Continuous Improvement

ServeusAI is committed to the continuous improvement of its information security program.

Security controls, policies and operational procedures are reviewed and enhanced where appropriate to address evolving risks, technological developments and customer expectations.

ANNEX III

Approved Subprocessors

This Annex forms an integral part of the Data Processing Agreement ("DPA") and identifies the Subprocessors authorized by ServeusAI to Process Customer Personal Data in connection with the provision of the Services.

ServeusAI remains responsible for the acts and omissions of its Subprocessors to the extent required by Applicable Data Protection Laws and shall ensure that each Subprocessor is bound by written contractual obligations providing a level of protection for Customer Personal Data that is no less protective than those set out in this DPA.

The list below reflects the Subprocessors engaged by ServeusAI as of the Effective Date of this DPA.

Current Approved Subprocessors

Subprocessor	Purpose	Processing Activities	Primary Processing Region
Microsoft Azure	Cloud infrastructure and hosting	Hosting, storage, networking, backup, infrastructure security and related cloud platform services	European Economic Area
OpenAI	Artificial intelligence services	AI-assisted document analysis and information extraction	As configured by ServeusAI and subject to the applicable OpenAI Data Processing Addendum
Anthropic	Artificial intelligence services	AI-assisted document analysis and information extraction	As configured by ServeusAI and subject to the applicable Anthropic Data Processing Addendum

Cloudflare	Network and application security	Content delivery, network protection, traffic management and security services	Global network, processed in accordance with applicable Cloudflare data processing commitments
Google Workspace	Business productivity and customer support	Email, collaboration and customer communications where required for support activities	As described in Google's applicable Data Processing Terms

Engagement of Subprocessors

ServeusAI may engage additional Subprocessors where reasonably necessary to provide, maintain, secure or improve the Services.

Before engaging a new Subprocessor that will Process Customer Personal Data, ServeusAI shall implement appropriate contractual, technical and organizational safeguards consistent with Applicable Data Protection Laws.

Where required by the Agreement or Applicable Data Protection Laws, Customers shall receive reasonable advance notice of material changes to the list of Subprocessors.

Customer Objections

Where Applicable Data Protection Laws grant the Customer the right to object to the appointment of a new Subprocessor, the Customer may submit a written objection within thirty (30) days after receiving notification.

The objection shall include reasonable grounds relating to data protection or information security concerns associated with the proposed Subprocessor.

The Parties shall cooperate in good faith to identify a commercially reasonable solution.

Where no reasonable solution can be reached, either Party may terminate only the affected Services in accordance with the Agreement.

Subprocessor Requirements

Before authorizing a Subprocessor to Process Customer Personal Data, ServeusAI shall ensure that the Subprocessor:

- is subject to appropriate due diligence;
 - enters into a written agreement containing data protection obligations consistent with Article 28 GDPR;
 - implements appropriate technical and organizational measures designed to protect Customer Personal Data;
 - Processes Customer Personal Data only on documented instructions received from ServeusAI; and
 - supports ServeusAI in fulfilling its obligations under the DPA where applicable.
-

International Data Transfers

Where a Subprocessor Processes Customer Personal Data outside the European Economic Area, the United Kingdom or Switzerland, ServeusAI shall ensure that such Processing is subject to an appropriate transfer mechanism recognized under Applicable Data Protection Laws, including where appropriate:

- an adequacy decision;
- the European Commission Standard Contractual Clauses;
- the UK International Data Transfer Addendum; or
- another legally recognized transfer mechanism.