Keto

Data processing agreement

Keto Software Oy, Version: August 2025

info@
ketosoftware.com

Table of contents

Keto
Software

1. Preamble

This Data Processing Agreement ("DPA") is entered into between the Customer (as defined in the Keto License Agreement or Order Form) and:

Keto Software Oy
Kankurinkatu 4–6
05800 Hyvinkää, Finland
("Keto" or "Processor")

This DPA governs the processing of Personal Data by Keto on behalf of the Customer in connection with the provision of the Keto Services. It supplements the Keto License Agreement (KLA), Order Form, General Terms and Conditions (GTCs), and any related attachments (together, the “Agreement”).

Keto may process Customer Personal Data when delivering services under the Agreement. This DPA sets forth the parties' obligations in accordance with applicable Data Protection Laws, including the General Data Protection Regulation (EU) 2016/679 (GDPR) and other applicable legislation.

- Where the Customer is a Controller, Keto acts as a Processor.
- Where the Customer is a Processor, Keto acts as a Sub-Processor.

In the event of conflict between this DPA and other Agreement documents, this DPA shall prevail regarding data protection matters.

2. Definitions

Terms used in this DPA have the meanings set out in GDPR and relevant Data Protection Laws. Notable definitions include:

Personal Data: Any information relating to an identified or identifiable natural person.

Processing: Any operation performed on Personal Data, such as collection, storage, use, or deletion.

Data Subject: An individual whose Personal Data is processed.

Customer Data: All data submitted by the Customer or users to the Keto Platform, including Personal Data.

Keto
Software

Sub-Processor: Any third party appointed by Keto to assist in processing Customer Data. 4 / 13 Keto DPA

Data Protection Laws: GDPR, UK GDPR, Finnish Data Protection Act, and other applicable laws.

Adequate Jurisdiction: Countries with recognized data protection adequacy status under GDPR or equivalent regimes

3. Execution and Duration

This DPA becomes effective upon the Effective Date of the Agreement (specified in the KLA or Order Form). It remains in force for the duration of the Agreement and any data retention period, thereafter, as described below.

4. Responsibilities of the Customer (Data Controller)

The Customer shall:

- Ensure it has a valid legal basis for all Personal Data shared with Keto.
- Inform Data Subjects as required under Data Protection Laws.
- Maintain accuracy and lawfulness of Customer Data.
- Manage user permissions and data uploaded to the Keto platform.
- Respond to Data Subject requests where appropriate.

5. Responsibilities of Keto (Data Processor)

Keto shall:

- Process Personal Data solely per documented Customer instructions.
- Maintain data confidentiality.
- Limit access to personnel with appropriate training and authorization.
- Assist Customer with data subject rights and privacy impact assessments.
- Notify Customer of Personal Data breaches without undue delay (typically within 48 hours).
- Enable audits or supply third-party certification reports upon request (subject to reasonable limits and confidentiality).

Where the Customer enables optional AI+ functionality, certain Personal Data may be

transferred to Keto's sub-processors, including Microsoft Azure OpenAI Services, for the purpose of generating responses or processing user prompts, subject to the restrictions of this DPA. The Customer acknowledges and expressly agrees that enabling AI+ functionality may involve the processing of Personal Data by third-party sub-processors (e.g., Microsoft Azure OpenAI Services). The Customer retains the right to disable AI+ Services at any time without prejudice to its other contractual rights.

6. Optional AI+ Services

Where the Customer enables optional AI+ features, Keto may transmit Personal Data (e.g.user prompts or project data) to its sub-processor Microsoft Corporation (Azure OpenAI Services) solely for generating AI responses.

This processing is:

- Initiated exclusively by Customer/user input
- Subject to Microsoft's "Code of Conduct for Azure OpenAI Services"
- Not used to train or improve underlying AI models
- Logged, monitored, and secured in accordance with this DPA

The Customer retains full ownership and responsibility for input and output data associated with AI+.

7. Use of Sub-processors

Keto may engage Sub-processors for specific processing tasks. A current list is available in Exhibit B.

Keto will:

- Ensure Sub-processors are contractually bound to obligations equivalent to this DPA
- Notify the Customer in advance of any changes to Sub-processors
- Allow the Customer to object within 15 business days; in case of unresolved objections, the Customer may terminate only the affected services. In case of a Customer objection to a new Sub-Processor, the Parties shall in good faith discuss alternatives before the Customer exercises its right to terminate the affected services.

8. Hosting and Data Transfer

Depending on the Customer's selection in the Agreement, Customer Personal Data will be hosted on data servers located in the:

- European Economic Area (EEA)
- United Kingdom (UK)
- United States (US) (where applicable and selected)

Additionally, data may be processed at Keto's affiliated locations, including:

- Keto Software Ltd (London, UK)
- Keto Software AG (Zug, Switzerland)

Transfers to countries outside an Adequate Jurisdiction shall be made only in compliance with applicable Data Protection Laws, using appropriate safeguards such as Standard Contractual Clauses (SCCs).

9. Data Retention and Deletion

- The Customer may delete Customer Data at any time through the platform.
- Upon termination of the Agreement, Keto will, upon written request, provide a copy of Customer Data.
- Customer Data will be deleted from active systems within 90 days of termination, unless required for legal retention.
- Backup copies will be automatically deleted within 365 days. Backup copies shall be automatically deleted within one hundred eighty (180) days after termination of the Agreement, unless a longer retention period is required by applicable law.
- During retention, such data remains subject to the terms of this DPA.

10. Security Measures

Keto implements appropriate Technical and Organizational Measures (TOMs), described in Exhibit C, to ensure the security of processing. These include but are not limited to:

- Encryption at rest and in transit
- Logical access control and monitoring
- Secure backup and disaster recovery
- Security incident response protocols

11. Rights of Data Subjects

During the Term, Keto will enable the Customer to access, rectify, restrict, delete, or export Customer Personal Data through the functionalities of the Keto Services, where technically feasible.

If Keto receives a Data Subject Request directly (e.g., access, deletion, rectification), Keto will, to the extent legally permitted, promptly notify the Customer and redirect the Data Subject to submit the request directly to the Customer. Keto will not respond to such a request unless authorized by the Customer or required by law.

12. Audit Rights and Security Testing

The Customer may audit Keto's compliance with this DPA:

- Once per year or in case of a confirmed security incident,
- By providing 15 business days' written notice,
- Keto may provide certifications, audit reports, or documentation in lieu of onsite audits.
- In addition, the Customer shall be entitled to conduct an on-site audit in case of substantiated suspicion of non-compliance.

Penetration tests are permitted under the following conditions:

- Prior written approval of Keto (at least 5 business days in advance),
- Scope and methods agreed upon,
- No disruption to services or impact on other customers.

Physical penetration testing of hosting infrastructure (e.g., GCP data centers) is strictly prohibited.

Keto shall provide reasonable assistance to the Customer in fulfilling its obligations under applicable Data Protection Laws to respond to such requests, taking into account the nature of the Processing and the information available to Keto.

13. Liability

Liability for each Party is governed by the limitations defined in the Agreement (KLA, or Order Form and GTCs). Nothing in this DPA expands either Party's liability beyond the agreed contractual limits. Nothing in this Section shall limit either Party's liability for breaches of applicable data protection laws or for regulatory fines imposed directly by competent supervisory authorities.

14. Final Provisions

Severability
If any provision of this DPA is held invalid, the remaining provisions remain in full force. The invalid term shall be replaced by a valid term closest in meaning and purpose.

Governing Law and Jurisdiction
This DPA is governed by Finnish law. The competent courts of Helsinki, Finland shall have exclusive jurisdiction, unless otherwise agreed.

Exhibit A – Subject Matter and Details of Processing

Subject Matter:
Provision of the Keto Services, including AI+ features where enabled.

Duration:
Throughout the Agreement and up to deletion of Customer Data in accordance with this DPA.

Nature and Purpose of Processing:
Storing, transmitting, generating, and analysing Personal Data for purposes including:
- User authentication
- Platform operation and performance
- AI+ features (e.g., content generation, translation, project insights)

Categories of Personal Data:
- Name
- Email address
- Profile information (e.g., job title)
- Interaction and usage metadata
- AI+ prompts and responses (if feature enabled)
- Uploaded content (files, text, tags)

Categories of Data Subjects:
- Customer's employees and contractors
- Other authorized users accessing the Keto Services

Keto
Software

15. Exhibit B – Approved Sub-Processors

Third Party Provider

Below is the list of sub-processors authorized by Keto Software Oy to process Customer Personal Data in connection with the Keto Services. Each sub-processor is contractually bound to data protection obligations equivalent to those set out in this DPA.

Provider	Legal Name of provider	Address	Service Description
GOOGLE CLOUD	Google Cloud EMEA Limited	Velasco Clanwilliam Place Dublin 2 Ireland	Cloud hosting and infrastructure
Azure Open AI Services	Microsoft Irland Operations Ltd	One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521 Ireland	AI model hosting (Azure OpenAI, EU-hosted)
DeepL	DeepL	DeepL SE Maarweg 165 50825 Cologne Germany	Translation Services
Oivan	Oivan Group Oy, Oivan Finland Oy	Ruoholahdenkatu 8 00180 Helsinki Finland	Server Hosting partner for Middle East Clients

Affiliates

Provider	Legal Name of provider	Address	Service Description
Keto Switzerland	Keto Software AG	Kolinplatz 5 6300 Zug Switzerland	Support Services
Keto UK	Keto Software Ltd.	385-389 Oxford Street W1C 2NB London UK	Support Services

Keto
Software

16. Exhibit C – Technical & Organisational Measures

Information Security Program
Keto implements an Information Security Management System (ISMS) certified under ISO/IEC 27001. This system governs all relevant aspects of security in line with industry standards. Measures are evaluated and updated regularly to ensure data protection and operational resilience.

Audits and Certifications
Keto maintains ISO 27001 certification and may provide proof of compliance or relevant third-party audit summaries upon request, under confidentiality.

Hosting & Infrastructure
Keto services are hosted via Google Cloud Platform (GCP) in data centers located in Hamina (Finland) or London (UK), which are ISO 27001, 27017, 27018 and SOC 1/2/3 certified. Hosting infrastructure includes:
- Physical access restrictions (biometrics, surveillance, intrusion detection)
- Logical separation of customer environments
- TLS encryption for network traffic
- Data encryption at rest

Encryption
- In Transit: TLS 1.2 or higher for all data transfer.
- At Rest: AES 256-bit encryption of customer data within GCP infrastructure.

Access Control
- Role-based access control with the principle of least privilege
- MFA (multi-factor authentication) for privileged access
- Centralized identity and authorization management
- Logging and monitoring of access attempts

Data Separation
- Logical multi-tenancy: Each customer has a dedicated database and environment
- Test and production environments are separated
- Access to customer data is restricted to authorized personnel only

Confidentiality
All Keto employees are under confidentiality agreements. Only trained personnel with a need-to-know basis may access Personal Data. Security and data protection training is provided regularly.

Incident Management & Monitoring
- Continuous system monitoring
- Incident escalation and tracking procedures

- Critical issues handled with the highest development priority
- Breach notifications as per legal obligations (typically within 48 hours)

Vulnerability Management & Penetration Testing

- Regular vulnerability scans
- Annual third-party penetration tests
- Customers may request vulnerability testing under pre-agreed scope (see DPA terms)

Availability & Business Continuity

- Daily data backups, retained for 30 days
- Recovery Time Objective (RTO): 48 hours; Recovery Point Objective (RPO): 24 hours
- Annual Business Continuity and Disaster Recovery (BCDR) reviews
- High availability through GCP live migration and redundancy

Logging & Audit Trails

- System logs are maintained to track user activity and changes
- Logs are retained securely and used for security investigations and audits

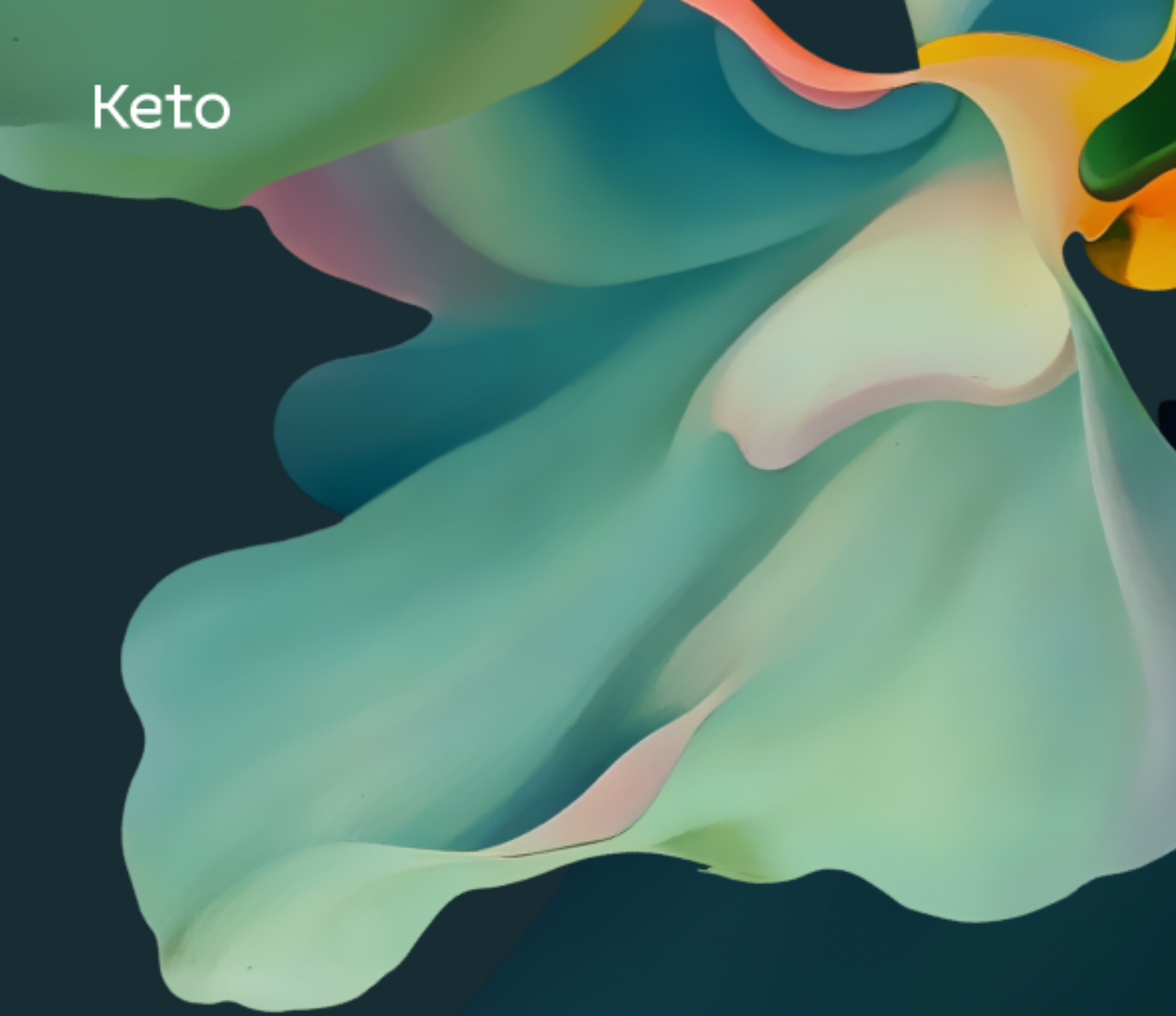
Data Minimization and Retention

- Customers control deletion of data via platform functionality
- Upon termination, data is deleted within 90 days (active systems); backups purged within 365 days
- Retained data is subject to confidentiality and secured storage

Organizational Measures

- Security governance framework with designated responsibilities
- Formal onboarding and offboarding processes
- Security policies reviewed and acknowledged by all employees

Keto



info@
ketosoftware.com