KONTANA OÜ DATA PROCESSING AGREEMENT (DPA)

Version: 2.0
Effective date: 11 August 2026
Part of: Kontana OÜ Accounting Service General Terms

This Data Processing Agreement (the **DPA**) governs the processing of personal data by Kontana OÜ on behalf of the Client in providing the accounting service. The DPA is an integral part of the Kontana OÜ accounting service agreement (the **Agreement**).

1. Parties and roles

1.1. The **Client** is a legal person registered in Estonia whose details are stated in the Agreement or the Portal. The Client is the controller for processing covered by the DPA.

1.2. **Kontana OÜ** (registry code 17278366, address A. H. Tammsaare tee 92, 13424 Tallinn, Estonia, email `hei@kontana.ee`) is the processor for processing covered by the DPA.

1.3. Kontana is an independent controller when it processes personal data for purposes determined by Kontana to administer the Agreement, bill for the Service, ensure the security of the Portal and Service, prevent fraud, protect legal claims, carry out anti-money laundering and sanctions checks, or comply with another legal obligation applicable to Kontana. The DPA does not apply to that processing; Kontana is responsible for its legal basis, retention period, security and required notices.

1.4. Terms defined in Regulation (EU) 2016/679 (the **GDPR**) have the same meaning in the DPA. If the DPA conflicts with another Agreement document, the DPA prevails on personal data processing matters.

2. Duration and instructions

2.1. The DPA takes effect with the Agreement and continues until Kontana has returned or deleted all personal data processed on behalf of the Client. If Kontana retains accounting records on the Client's instructions after the Service ends, the DPA continues until that retention ends.

2.2. Kontana processes personal data only on the Client's documented instructions. The Agreement, the service plan selected by the Client, the Portal settings, and instructions given by the Client in writing or in a form that can be reproduced in writing are documented instructions.

2.3. If a new instruction falls outside the agreed scope of the Service, the Parties will agree on technical feasibility and any additional fee before it is carried out. Kontana will

immediately inform the Client if, in its opinion, an instruction infringes the GDPR or other applicable data protection law.

3. Kontana's obligations as processor

Kontana:

3.1. processes personal data only on documented instructions, including in relation to transfers outside the European Economic Area (**EEA**), unless processing is required by EU or Estonian law;

3.2. ensures that personal data is accessible only to persons who need access to provide the Service and who are subject to a contractual or statutory duty of confidentiality;

3.3. implements the technical and organisational security measures in Appendix 2 appropriate to the risks of the processing;

3.4. notifies the Client of a personal data breach without undue delay and, where possible, within 36 hours after becoming aware of it. Kontana provides the information then available on the nature and likely consequences of the breach, affected data and persons, and mitigation measures taken; missing information may be provided in phases;

3.5. reasonably assists the Client in responding to data subject requests and complying with obligations under Articles 32–36 of the GDPR, including breach assessments, data protection impact assessments and prior consultation with a supervisory authority;

3.6. maintains records of processing activities under Article 30(2) of the GDPR and makes available to the Client the information necessary to demonstrate compliance with the DPA;

3.7. does not sell personal data processed on the Client's behalf, use it for Kontana's own marketing or to train general-purpose artificial intelligence models, or process it for another purpose unrelated to the Client's instructions;

3.8. informs the Client of the legal basis before complying with a processing requirement imposed by law unless the law prohibits that notification.

4. Client's obligations as controller

The Client:

4.1. ensures that there is a valid legal basis for collecting, disclosing to Kontana and processing personal data under the DPA and that the required information has been given to data subjects;

4.2. gives Kontana lawful, sufficiently clear and documented instructions and is responsible for those instructions and for the accuracy of data supplied to Kontana;

4.3. does not submit personal data to the Service that is not reasonably necessary to provide the Service and informs Kontana if processing requires stronger-than-usual security measures;

4.4. is responsible for its users, access rights and authentication methods and for substantively resolving data subject requests;

4.5. decides, in accordance with section 8 when the Agreement ends, whether accounting records are transferred or retained by Kontana until the statutory retention period expires.

5. Sub-processors

5.1. The Client gives Kontana general authorisation to use the sub-processors listed in Appendix 3. Kontana may use a sub-processor only to the extent necessary to provide the Service.

5.2. Kontana notifies the Client of an intended new or replacement sub-processor at least 15 calendar days in advance by email or through the Portal. If urgent replacement is required by a security, reliability or legal risk, Kontana will notify the Client as soon as possible.

5.3. The Client may object to a new sub-processor on reasonable data protection grounds. The Parties will attempt to find a reasonable solution. If that is not possible, Kontana may discontinue the affected function or the Client may terminate the Agreement before the change takes effect.

5.4. Kontana enters into an agreement with each sub-processor that provides at least an equivalent level of data protection to the DPA and remains liable to the Client for processing carried out by the sub-processor on Kontana's behalf.

5.5. Kontana enters into and administers the agreements and accounts for the software services used to provide the Service, including Merit Aktiva and CostPocket. When processing data on the Client's behalf, those service providers are Kontana's sub-processors and are subject to the requirements of this section.

6. International data transfers

6.1. Kontana prefers to store and process personal data processed on behalf of the Client in the EEA. Data may be transferred outside the EEA only under a mechanism compliant with Chapter V of the GDPR, such as a European Commission adequacy decision, the Data Privacy Framework or standard contractual clauses, and with supplementary safeguards where necessary.

6.2. Azure OpenAI is used in a configuration with EU data residency. Kontana does not use a global deployment for Client data that permits inputs or outputs to be processed outside

the EU without informing the Client in advance and ensuring an appropriate transfer mechanism.

6.3. Appendix 3 states the known principal processing region and applicable transfer mechanism. Support or administrative access from outside the EEA is treated as an international transfer even if the data is hosted in the EEA.

7. Audit and demonstration of compliance

7.1. At the Client's reasonable request, Kontana provides the information necessary to assess compliance with the DPA, including relevant descriptions of security measures and summaries of any independent audits or certifications.

7.2. If the information provided is insufficient, the Client may audit processing covered by the DPA itself or through an independent auditor subject to confidentiality. The Client gives at least 30 calendar days' notice and conducts the audit during working hours in a manner that does not unreasonably disrupt Kontana's or other clients' services. The notice period does not apply following a material security incident or a request from a supervisory authority.

7.3. The Client bears the audit costs unless the audit identifies a material breach of the DPA by Kontana, in which case Kontana bears its own reasonable audit and remediation costs.

8. Return of data and statutory retention

8.1. The Client is an accounting entity and is responsible for compliance with the retention obligations in section 12 of the Estonian Accounting Act. Through the DPA, the Client gives Kontana the documented instruction to retain accounting records processed as part of the Service until the applicable statutory retention period expires, generally seven years after the end of the financial year in which the transaction was recorded in the accounting records. During that period, Kontana processes the records only for secure retention, making them available to the Client, and supporting activities required by law.

8.2. When the Agreement ends, the Client may choose whether:

- Kontana continues to retain the accounting records until the end of the period stated in section 8.1; or
- Kontana transfers the records to the Client or its authorised new service provider and deletes its copies after the Client confirms that statutory retention is otherwise ensured.

If the Client wants immediate transfer and deletion, it must give that instruction within 30 days after the Agreement ends. If no instruction is given, Kontana continues retaining the accounting records as described in section 8.1. The Client may also request transfer and deletion of Kontana's copies later during the retention period if it confirms that statutory retention is otherwise ensured. The DPA continues until retention ends.

8.3. Ordinary retention under section 8.1 and reasonable access to and a standard export of accounting records during the retention period are included in the Service fee. Non-standard conversion or substantial manual work may be charged separately under the General Terms if Kontana states the price or the basis for calculating it before carrying out the work.

8.4. At the Client's choice, Kontana returns or deletes personal data not forming part of the accounting records described in section 8.1 no later than 90 days after the Agreement ends. Data in backups is deleted during the ordinary backup cycle and is not used for another purpose or restored except where required for security or business continuity.

8.5. This section does not govern data retained by Kontana as an independent controller under section 1.3. Such data is retained only to the extent required by the applicable purpose and legal basis.

9. Liability

9.1. Each Party is liable for damage caused by its own infringement of the GDPR or the DPA to the extent attributable to that Party. The Parties cooperate in resolving data subject claims and supervisory proceedings.

9.2. Section 7 of the General Terms applies to liability between the Parties, including provisions on direct loss, the liability cap and exceptions to limitations of liability. The DPA does not limit the statutory rights of a data subject or supervisory authority or the Parties' liability to the extent it cannot be limited by law.

9.3. If a Party incurs a cost due to a third-party claim, administrative fine or other measure, the other Party reimburses it only to the extent caused by that other Party's breach and to the extent reimbursement is permitted by law.

10. Final provisions

10.1. The provisions of the General Terms on amendments, notices, governing law and dispute resolution apply to the DPA.

10.2. Termination of the DPA does not terminate provisions which by their nature must continue after processing ends, including provisions on confidentiality, deletion, audit and liability.

10.3. The DPA is published in Estonian and English. If the language versions conflict, the Estonian text prevails.

Appendix 1. Description of processing

Category	Description
Purpose	Providing the agreed accounting service, including processing documents and bank transactions, maintaining accounting records, payroll, tax returns, annual reports, client support and data archiving.
Operations	Collection, receipt, entry, organisation, structuring, comparison, correction, use, disclosure on the Client's instructions, retention, export and deletion.
Data subjects	The Client's management board members, employees, contractors, customers, suppliers, contact persons, beneficiaries and other natural persons named in the Client's documents.
Personal data	Name, personal identification code or date of birth, contact and employment information, role and authority to represent, invoices, receipts, agreements, bank account and payment data, transaction data, payroll and tax data, user and access data, and other information contained in documents.
Special categories	Payroll, absence, reimbursement or other source documents may contain limited health, trade union or other special-category information. Criminal offence data is processed only if contained in a document supplied by the Client and the processing is lawful.
Frequency	Continuous or recurring processing depending on the Client's use and reporting periods.
Duration	The term of the Agreement and a transfer period of up to 90 days; for accounting records, the statutory retention period described in section 8.

Appendix 2. Technical and organisational security measures

Taking into account the nature, scope and risks of processing, Kontana implements measures including:

1. **Access control:** individual user accounts; role-based access and least privilege; multi-factor authentication for privileged and production access; regular access reviews; and prompt revocation of rights.

2. **Encryption:** TLS 1.2 or later for data in transit; encryption of stored data and backups using the cloud provider's standard strong encryption, generally equivalent to AES-256.

3. **Separation and minimisation:** logical separation of client data and separation of production, development and test environments; avoiding the use of real personal data in testing unless necessary and additionally protected.

4. **Logging and monitoring:** logging of security, access and material administrative activities; monitoring and alerts for relevant anomalies; and restricted access to logs. Personal data is not knowingly included in error reports or logs beyond what is needed to resolve an issue.

5. **Backup and continuity:** regular automated backups, protection of backups, periodic restoration checks, and documented incident and recovery processes.

6. **Secure development:** change review; dependency and vulnerability monitoring; risk-based deployment of security patches; secure secrets management; and periodic security testing, including independent testing where appropriate.

7. **Use of artificial intelligence:** only data necessary for the task is sent to an AI service; Azure OpenAI is used with EU data residency; and Client inputs and outputs are not used to train general-purpose models.

8. **Personnel:** confidentiality obligations; data protection and information security training on joining and periodically thereafter; and documented access-granting and offboarding processes.

9. **Sub-processor oversight:** assessment of data protection and security terms before a service is introduced and risk-based follow-up assessments; agreements compliant with Article 28 of the GDPR; and safeguards for international transfers.

10. **Data lifecycle:** application of retention periods, export and deletion processes, and permanent deletion or anonymisation after the purpose and retention period end.

Appendix 3. Sub-processors and integrated services

Service provider	Service and data processed	Principal region / transfer mechanism	Role
Amazon Web Services EMEA Sàrl	S3 object storage, virtual servers and infrastructure; Client documents, application data and backups.	Stockholm, Sweden (`eu-north-1`), EEA.	Sub-processor.
Microsoft Ireland Operations Limited (Azure OpenAI Service)	Artificial intelligence inference; inputs and outputs necessary for the task.	Sweden, EU; EU data residency.	Sub-processor. Data is not disclosed to OpenAI or used to train general-purpose models.
Merit Tarkvara AS (Merit Aktiva)	Accounting records, invoices, payment, payroll and reporting data.	Estonia, EEA.	Sub-processor.
CostPocket OÜ	Collection, digitisation and transfer of expense and purchase documents.	Estonia; the service's own sub-processors may process data in other countries subject to applicable safeguards.	Sub-processor.

Service provider	Service and data processed	Principal region / transfer mechanism	Role
Mailgun Technologies, Inc. (Sinch Email)	Sending transactional emails and invoices; sender and recipient data, message content, attachments and delivery metadata.	Mailgun EU region; message data remains in the EU region. Limited account and administrative data may be processed in the United States under the EU-US Data Privacy Framework and/or standard contractual clauses.	Sub-processor.
Entusiastid OÜ (OAuth.ee)	User authentication; name, personal identification code, email address and/or phone number necessary for authentication and technical authentication data.	Estonian service provider; OAuth.ee processes authentication data temporarily during authentication. Any international transfer is subject to section 6.	Sub-processor.

Kontana keeps the list up to date and gives notice of changes as described in section 5.2.