

KONTANA OÜ PRIVACY POLICY

Version: 2.2

Effective date: 2 September 2026

Related documents: Kontana OÜ Accounting Service General Terms and Data Processing Agreement

1. Scope and contact

This Privacy Policy explains how Kontana OÜ (registry code 17278366, address A. H. Tammsaare tee 92, 13424 Tallinn, Estonia; **Kontana**) processes personal data in connection with the website kontana.ee, the web application app.kontana.ee (the **Portal**) and the accounting service.

For data protection questions and to exercise your rights, contact Kontana at hei@kontana.ee.

2. Kontana's role

Kontana is a controller principally for Client representatives' and users' account, authentication, communication and billing data and for data relating to the security of the Service and Portal, fraud prevention, legal claims, anti-money laundering and sanctions checks.

When Kontana processes personal data contained in the Client's accounting records on the Client's behalf, the Client is the controller and Kontana is the processor. That processing is governed by the Data Processing Agreement (**DPA**), and the Client determines its purposes and legal bases.

3. Data, sources, purposes and legal bases

Data and sources	Purpose	Legal basis
Client representative's and user's name, work contact details, company, role, authority to represent, and account and communication data; obtained from the person, the Client or a public register.	Establishing and managing the client relationship, Portal account, providing the Service and communicating.	Kontana's legitimate interest in performing its agreement with the Client and managing a B2B client relationship (Article 6(1)(f) GDPR).
Identification data necessary for authentication obtained from OAuth.aa, such as name, personal identification code, email address or phone number, and technical authentication data.	User authentication, verification of authority to represent, and account and Service security.	Legitimate interest (Article 6(1)(f)) and, where an applicable obligation exists, legal obligation (point (c)).
Identification, representation, activity, risk profile, PEP and sanctions screening data concerning the Client, its representative and beneficial owner; obtained from the Client, the commercial register and other reliable sources.	Anti-money laundering, counter-terrorist financing and sanctions compliance.	Legal obligation (Article 6(1)(c)).
Agreement, order, invoice and payment data.	Billing, Kontana's accounting and administration of contractual rights and obligations.	Legal obligation (Article 6(1)(c)) and legitimate interest (point (f)).
IP address and limited website request metadata; Portal device, session, usage, security and activity data.	Website and Service operation; network and information security; troubleshooting; abuse and fraud prevention; limited aggregate website measurement; protection of legal claims.	Legitimate interest (Article 6(1)(f)) and, where necessary, legal obligation (point (c)).
Marketing contact details and preferences.	Sending news and offers.	Consent (Article 6(1)(a)) or, where permitted by law, legitimate interest (point (f)); messages can be opted out of at any time.
Consented paid-ad attribution data: advertising platform, landing-page path, campaign parameters, platform-specific click identifier, consent version and language, and application or possible joining outcome; obtained from the landing-page address, the applicant and client-relationship data.	Analysing Kontana's advertising performance and reporting an application submission or joining to the platform that referred the visit.	Consent (Article 6(1)(a)).
Accounting records and data in them obtained from the Client, integrations or accounting software.	Accounting service and archiving ordered by the Client.	Kontana processes the data as a processor under the Client's documented instructions and the DPA.

3.1 Website request data

For the public website, Kontana records limited security request metadata: IP address, request timestamp, HTTP method, requested path without its query string, response status and size, request duration, host, User-Agent, referrer domain and request ID. Kontana uses it to deliver and operate the website, maintain network and information security, detect malicious or abnormal traffic, investigate attacks and technical incidents, and prevent repeated abuse. The legal basis is Kontana's legitimate interest in protecting the website, systems and information security (Article 6(1)(f)).

Kontana also reduces request information into hourly aggregate statistics to understand approximate traffic trends, distinguish declared bots from human-or-unknown traffic, understand broad mobile, tablet and desktop use and referring domains, and monitor page availability and response errors. The statistics contain no IP addresses, full User-Agents, full referrer URLs, query strings, unique visitor or session identifiers, or hashes derived from visitor information. They are not intended to identify visitors and measure page loads rather than unique individuals. Bots that present an ordinary browser User-Agent may remain in the human-or-unknown figures.

For this measurement, the public website uses no analytics JavaScript, tracking pixels, browser storage, analytics cookies or fingerprinting and does not try to follow a visitor between visits. The legal basis is Kontana's legitimate interest in understanding broad website use and maintaining a functional, appropriately operated website (Article 6(1)(f)), balanced by the absence of persistent identifiers and the rapid reduction of request data into aggregate statistics.

Kontana does not make decisions based solely on automated processing that produce legal or similarly significant effects for a data subject. Kontana may use automation and artificial intelligence to provide the Service, but remains responsible for properly performing the agreed accounting work. Automated Portal replies are not standalone tax, legal or business advice unless marked as confirmed by a Kontana accountant.

3.2 Advertising performance measurement

When a visitor reaches Kontana's website from a paid Google Ads, LinkedIn or Meta advertisement and gives voluntary consent in the form, Kontana stores with the application the advertising platform, landing-page path, campaign parameters, platform-specific click identifier, consent version and language, and information about the application submission and possible later joining.

Kontana uses this data to analyse the performance of its advertising. Kontana may send the click identifier and the application-submission or joining event and time to the platform that referred the visit so the platform can associate the outcome with the relevant advertisement. The application content, company data, email address and other contact details are not sent for this purpose.

The legal basis for this processing is consent (Article 6(1)(a) GDPR). Refusing consent does not affect submission or review of the application. Consent can be withdrawn at any time by contacting hei@kontana.ee. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

4. Service providers and other recipients

Service provider	Use
Amazon Web Services EMEA Sàrl	S3 object storage, virtual servers, backups, public website security request logs and aggregate traffic statistics in the Stockholm region (eu-north-1).
Microsoft Ireland Operations Limited	Azure OpenAI artificial intelligence inference in Sweden with EU data residency. 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.
CostPocket OÜ	Collection, digitisation and transfer of expense and purchase documents.
Mailgun Technologies, Inc. (Sinch Email)	Sending transactional emails and invoices from Mailgun's EU region.
Entusiastid OÜ (OAuth.ee)	User authentication; OAuth.ee processes authentication data temporarily during authentication.
Google Ireland Limited (Google Ads), LinkedIn Ireland Unlimited Company and Meta Platforms Ireland Limited	Advertising performance measurement based only on voluntary consent. Data is sent only to the platform that referred the consented visit.

Kontana discloses data only to the extent necessary to provide the Service, carry out the Client's instructions or comply with a legal obligation. On the Client's instructions, Kontana may also disclose data to banks, e-invoice operators, auditors or other recipients, and where required by law to the Estonian Tax and Customs Board, the Financial Intelligence Unit, a court or another competent authority. The current list of sub-processors and more detailed information are in Appendix 3 to the DPA.

5. International transfers

Kontana keeps the principal processing of Client production data in the European Economic Area (**EEA**). If a service provider's limited support or administrative access or other processing involves a transfer outside the EEA, Kontana relies on a mechanism under Chapter V of the GDPR, such as a European Commission adequacy decision, the EU-US Data Privacy Framework or standard contractual clauses, and uses supplementary safeguards where necessary.

6. Retention

Kontana retains data only for as long as necessary for the applicable purpose or to comply with a legal obligation:

- On the Client's instructions and under the DPA, the Client's accounting records are generally retained for seven years after the end of the financial year in which the transaction was recorded in the accounting records. The transfer, archiving and access arrangements in the DPA apply when the Agreement ends.
- Kontana's own accounting source documents are generally retained for seven years after the end of the financial year applicable to them.

- Customer due diligence data collected for anti-money laundering purposes is retained for the period set by the Estonian Money Laundering and Terrorist Financing Prevention Act, generally five years after the business relationship ends.
- Client relationship, account and communication data is retained during the Agreement and afterwards to the extent necessary for closing the relationship, protecting legitimate claims or complying with a legal obligation. Data processed on behalf of the Client that is not part of archived accounting records is generally returned or deleted under the DPA within 90 days after the Agreement ends.
- Routine public website security request logs are normally deleted after 30 days. Information connected to a specific security incident may be retained longer where necessary to investigate the incident, prevent recurrence, comply with applicable obligations, or establish or defend legal claims. Hourly aggregate website statistics are retained for 24 months.
- Marketing data used to send news and offers is retained until consent is withdrawn or an objection is made and, to the necessary extent, to evidence the opt-out.
- Advertising attribution data that can be associated with a person is retained until consent is withdrawn, but no longer than 12 months after the application is submitted. Kontana may then retain only anonymised aggregate statistics.

Data in backups is deleted during the ordinary backup cycle and used only for security or business continuity purposes.

7. Security

Kontana applies technical and organisational measures appropriate to the risks of processing, including encryption in transit, role-based access and least privilege, multi-factor authentication for privileged and production access, separation of client data and environments, security logging and monitoring, protected backups and restoration checks, secure development and vulnerability management processes, personnel confidentiality and training obligations, service provider oversight, and data retention and deletion processes. A more detailed description is in Appendix 2 to the DPA.

8. Data subject rights

Where applicable, a data subject has the right to:

- obtain information and a copy of their personal data;
- have inaccurate data corrected;
- request deletion or restriction of processing;
- object to processing based on legitimate interests;
- withdraw consent at any time;
- receive data they provided in a machine-readable format and transmit it to another service provider where the right to data portability applies;
- lodge a complaint with the Estonian Data Protection Inspectorate (info@aki.ee, Tatari 39, 10134 Tallinn, aki.ee).

Send requests to hei@kontana.ee. Kontana normally responds within one month. If a request concerns data processed by Kontana on the Client's behalf, it is principally handled by the Client as controller and Kontana assists the Client under the DPA.

9. Cookies

The public website does not use analytics cookies or other browser storage for traffic measurement. The Portal uses cookies that are necessary to function and remain secure. Analytics or other non-essential cookies would be used only with consent.

10. Changes and languages

Kontana may update this Privacy Policy if the Service, processing or law changes. Where possible, material changes will be communicated in a reasonable manner before they take effect. The current version is published at kontana.ee, and historical versions are available in Kontana's GitHub repository.

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