

Privacy Policy

Aelethion OÜ

Last updated: 19 August 2026

Effective date: 19 August 2026

1. Who We Are

This Privacy Policy applies to Aelethion OÜ, a private limited company registered in Estonia (registry code: 17529868), with its registered address at Mäealuse tn 2/4, Mustamäe linnaosa, Tallinn, Harju maakond, 12618, Estonia ("Aelethion", "we", "us", "our").

Aelethion operates the Athena platform, a secure workspace in which a customer's personnel and AI agents carry out work under the customer's control, accessible at aelethion.com and related subdomains (collectively, the "Service").

For all data protection matters, you may contact us at:

Data Controller Contact: Email: Postal address: Mäealuse tn 2/4, Mustamäe linnaosa, Tallinn, Harju maakond, 12618, Estoniaprivacy@aelethion.com

We are registered as a data controller under the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the Estonian Personal Data Protection Act (isikuandmete kaitse seadus).

The supervisory authority responsible for overseeing our compliance is the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon): Website: www.aki.ee Address: Tatari 39, 10134 Tallinn, Estonia Email: info@aki.ee

2. Scope of This Policy

This Privacy Policy explains:

- What personal data we collect about you
- Why we collect it and on what legal basis
- How we use it
- Who we share it with
- How long we retain it
- Your rights under the GDPR

- How to contact us or lodge a complaint

This Policy applies to:

- Visitors to our website
- Users who register for a free or paid account on the Athena platform
- Business customers who use Athena to carry out work
- Individuals who contact us by email, form, or any other channel
- Individuals whose data may be present in material submitted to Athena for processing

This Policy does not apply to data processed by our customers in their own systems. When our customers use Athena to process their users' data, those customers are the data controllers and we act as their data processor. In that capacity, our obligations are governed by the Data Processing Agreement (DPA) we enter into with each customer, as required under GDPR Article 28.

3. Personal Data We Collect

3.1 Data You Provide Directly

Account registration: When you create an account, we collect your name, email address, company name (if applicable), and the password you set (stored in hashed form only).

Payment information: When you subscribe to a paid plan, payment is processed by our third-party payment processor. We do not store full card numbers or bank account details. We retain only the last four digits of your card, card type, billing name, and billing address for invoice purposes.

Contact and support: When you contact us by email or a contact form, we collect your name, email address, and the content of your message.

Communications preferences: If you subscribe to product updates or marketing communications, we collect your email address and your stated preferences.

3.2 Data We Collect Automatically

Usage data: When you use the Service, we collect information about your interactions, including pages visited, features used, tasks initiated, timestamps, and error logs. This helps us maintain, improve, and secure the Service.

Technical data: We collect your IP address, browser type and version, operating system, device identifiers, referring URLs, and session duration. This data is used for security monitoring, fraud prevention, and service analytics.

Cookies and similar technologies: We use cookies and similar tracking technologies as described in Section 9 of this Policy.

3.3 Data Within Customer Material

When a customer submits material to Athena for processing, that codebase may incidentally contain personal data, including names in comments, email addresses in configuration files, credentials, or other identifiers. We process this data solely to provide the audit service and do not use it for any other purpose. We do not retain Customer Data beyond the period necessary to complete the requested analysis, as described in Section 7.

4. Legal Bases for Processing

We process your personal data only where we have a valid legal basis under GDPR Article 6. The legal basis applicable to each processing activity is set out below.

Processing Activity	Legal Basis	GDPR Reference
Creating and managing your account	Performance of a contract	Art. 6(1)(b)
Providing the Athena service	Performance of a contract	Art. 6(1)(b)
Processing payments	Performance of a contract	Art. 6(1)(b)
Sending transactional emails (receipts, alerts, security notices)	Performance of a contract	Art. 6(1)(b)
Responding to support and enquiry requests	Legitimate interests	Art. 6(1)(f)
Security monitoring and fraud prevention	Legitimate interests	Art. 6(1)(f)
Website analytics and service improvement	Legitimate interests	Art. 6(1)(f)
Sending marketing communications to existing customers	Legitimate interests	Art. 6(1)(f)
Sending marketing	Consent	Art. 6(1)(a)

Processing Activity	Legal Basis	GDPR Reference
communications to new prospects		
Compliance with legal obligations (e.g. tax record retention)	Legal obligation	Art. 6(1)(c)

Where we rely on legitimate interests, we have assessed that our interests do not override your fundamental rights and freedoms. You may request a copy of our Legitimate Interests Assessment by contacting us at privacy@aelethion.com.

Where we rely on consent, you have the right to withdraw that consent at any time without affecting the lawfulness of processing carried out before withdrawal.

5. How We Use Your Personal Data

To provide and operate the Service: We use your account data and usage data to create and manage your account, process your subscription, deliver audit results, and provide customer support.

To improve the Service: We analyse aggregated, anonymised usage data to understand how the Service is used, identify bugs, and develop new features. We do not use Customer Data for model training or product improvement without your explicit consent.

To communicate with you: We send you transactional emails related to your account (receipts, security alerts, audit completion notices). If you have opted in, we may also send you product updates, feature announcements, and relevant content. You can unsubscribe from marketing communications at any time via the unsubscribe link in any email or by contacting us directly.

To ensure security and prevent fraud: We monitor usage patterns and access logs to detect suspicious activity, protect against unauthorised access, and investigate potential breaches.

To comply with legal obligations: We retain certain records as required by Estonian and EU law, including financial and tax records.

6. Sharing Your Personal Data

We do not sell your personal data. We do not share your personal data with third parties for their own marketing purposes.

We share personal data only in the following circumstances:

Service providers (data processors): We engage third-party providers who process personal data on our behalf to operate the Service. These include cloud infrastructure providers, payment processors, email delivery services, and analytics tools. All processors are bound by data processing agreements that require them to process data only on our documented instructions, maintain appropriate security measures, and comply with GDPR.

Our current sub-processors include:

Provider	Purpose	Location
[INSERT CLOUD PROVIDER, e.g. Hetzner / AWS / Nebius]	Infrastructure and hosting	[EU / EEA]
Stripe (or [INSERT PAYMENT PROCESSOR])	Payment processing	EU / USA (SCCs)
[INSERT EMAIL PROVIDER, e.g. Postmark]	Transactional email delivery	[EU / USA]
[INSERT ANALYTICS PROVIDER, e.g. Plausible]	Website analytics	[EU]

You may request an up-to-date list of sub-processors by contacting privacy@aelethion.com.

Legal requirements: We may disclose personal data if required to do so by law, regulation, or court order, or where necessary to protect the rights, property, or safety of Aeletion, our users, or others.

Business transfers: If Aeletion is involved in a merger, acquisition, or sale of assets, personal data may be transferred as part of that transaction. We will notify affected users in advance and ensure that the receiving party is bound by obligations no less protective than this Policy.

With your consent: We may share your data in other ways if you have given us specific consent to do so.

7. Data Retention

We retain personal data only for as long as necessary for the purposes for which it was collected, or as required by law.

Data Category	Retention Period
Account data (name, email, company)	Duration of account plus 3 years after account closure
Audit job metadata (timestamps, job IDs, results summaries)	Duration of subscription plus 2 years
Customer Data submitted for processing	Deleted upon job completion, maximum 24 hours after submission
Payment and billing records	7 years (Estonian Accounting Act requirement)
Support and correspondence records	3 years from last interaction
Marketing consent records	Until consent is withdrawn, plus 1 year
Security and access logs	12 months

When retention periods expire, we securely delete or anonymise the data. Where anonymisation is not technically feasible, we apply appropriate access controls and restrict further processing.

8. International Data Transfers

Aelethion is incorporated in Estonia and primarily processes data within the European Economic Area (EEA). Where we use sub-processors located outside the EEA (for example, certain payment processors or email delivery services), we ensure that appropriate safeguards are in place for international data transfers, including:

- Standard Contractual Clauses (SCCs) adopted by the European Commission
- Transfers to countries with an adequacy decision from the European Commission

You may request details of the transfer mechanisms applicable to specific sub-processors by contacting privacy@aelethion.com.

9. Cookies and Tracking Technologies

We use cookies and similar technologies on our website and platform. This section explains what we use and how you can control it.

Strictly necessary cookies: These cookies are required for the website and Service to function. They include session management cookies and security tokens. These cookies do not require your consent and cannot be disabled without affecting core functionality.

Analytics cookies: We use analytics tools to understand how visitors use our website. If we use analytics tools that set cookies, we will request your consent before placing them. You may withdraw consent at any time through our cookie preference centre.

Marketing and tracking cookies: We do not currently use advertising or retargeting cookies. If this changes, we will update this Policy and request your consent before placing any such cookies.

How to manage cookies: You may control cookies through:

- Our cookie consent banner, which appears on your first visit
- Your browser settings (note: disabling strictly necessary cookies may impair the Service)
- Our cookie preference centre, accessible at aelethion.com/cookies

In accordance with Estonian Electronic Communications Act requirements and the ePrivacy Directive, we obtain prior consent for all non-essential cookies before placing them. Consent records are stored and can be withdrawn at any time with the same ease as granting them.

10. Your Rights Under the GDPR

As a data subject under the GDPR, you have the following rights. You may exercise any of these rights by contacting us at privacy@aelethion.com. We will respond within 30 days. In complex cases, we may extend this period by a further two months and will notify you accordingly.

Right of access (Article 15): You have the right to request a copy of the personal data we hold about you and information about how we process it.

Right to rectification (Article 16): You have the right to request correction of inaccurate or incomplete personal data.

Right to erasure (Article 17): You have the right to request deletion of your personal data where it is no longer necessary for the purposes it was collected, where you withdraw consent (and there is no other legal basis), or where processing is unlawful.

Right to restriction of processing (Article 18): You have the right to request that we restrict processing of your personal data in certain circumstances, for example while the accuracy of data is contested.

Right to data portability (Article 20): Where processing is based on consent or contract and carried out by automated means, you have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller.

Right to object (Article 21): You have the right to object to processing based on legitimate interests or for direct marketing purposes. Where you object to direct marketing, we will stop processing immediately. Where you object on other grounds, we will stop unless we can demonstrate compelling legitimate grounds that override your interests.

Right to withdraw consent (Article 7(3)): Where processing is based on your consent, you may withdraw it at any time. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

Right not to be subject to automated decision-making (Article 22): We do not make decisions about you based solely on automated processing that produce legal or similarly significant effects. Audit results generated by Athena are provided as analytical outputs to inform human decision-making, not as automated decisions with legal effect.

Right to lodge a complaint: You have the right to lodge a complaint with the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) at www.aki.ee or with the supervisory authority in your EU Member State of habitual residence or place of work.

11. Security

We implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. These measures include:

- Encryption of personal data in transit (TLS 1.2 minimum) and at rest
- Access controls and role-based permissions limiting access to personal data to authorised personnel only
- Regular security testing and code review, including using our own tooling
- Incident response procedures and breach notification processes
- Staff training on data protection obligations

In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify the Estonian Data Protection Inspectorate within 72 hours of becoming aware of the breach, and will notify affected individuals without undue delay where required by GDPR Article 34.

12. Children's Privacy

The Service is not directed at children under the age of 16. We do not knowingly collect personal data from children under 16. If we become aware that we have collected personal data from a child under 16 without verified parental consent, we will delete that data promptly. If you believe we may have collected data from a child under 16, please contact us at privacy@aelethion.com.

13. Athena as a Data Processor

When business customers use Athena to carry out work, AeLeThion acts as a data processor on behalf of those customers, who are the data controllers in respect of any personal data within those customer environments.

In this capacity:

- We process Customer Data only on the documented instructions of the customer
- We do not use Customer Data for any purpose other than delivering the requested audit
- We delete Customer Data upon completion of the analysis job, within the retention period set out in Section 7
- We maintain appropriate technical and organisational security measures as required by GDPR Article 32
- We notify customers of any personal data breach affecting their Customer Data without undue delay
- We assist customers in responding to data subject requests relating to personal data within their systems
- We make available all information necessary to demonstrate compliance with GDPR Article 28

The terms governing our role as data processor are set out in the Data Processing Agreement (DPA) provided to business customers at the time of contracting. If you are a business customer and do not have a signed DPA in place, please contact privacy@aelethion.com.

14. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, the law, or the Service. When we make material changes, we will notify you by email (where we hold your email address) and by posting a prominent notice on our website at least 14 days before the changes take effect. The "Last updated" date at the top of this Policy reflects the most recent revision.

Your continued use of the Service after the effective date of any changes constitutes your acknowledgement of the updated Policy. If you do not agree to the updated Policy, you should stop using the Service and may request deletion of your account.

15. Contact Us

For any questions, requests, or concerns about this Privacy Policy or the way we handle your personal data, please contact us:

Aelethion OÜ Email: Postal address: Mäealuse tn 2/4, Mustamäe linnaosa, Tallinn, Harju maakond, 12618, Estonia privacy@aelethion.com

We aim to respond to all enquiries within 5 business days. For formal data subject rights requests, we will respond within 30 days as required by GDPR Article 12.

If you are not satisfied with our response, you have the right to lodge a complaint with the Estonian Data Protection Inspectorate:

Andmekaitse Inspektsioon (Data Protection Inspectorate) Website: www.aki.ee Email: info@aki.ee Address: Tatari 39, 10134 Tallinn, Estonia

This Privacy Policy was prepared in accordance with the General Data Protection Regulation (EU) 2016/679, the Estonian Personal Data Protection Act, and the Estonian Electronic Communications Act. It is governed by Estonian law.