

Privacy Policy

Version 2026-08-31 · Effective 31 August 2026

1. Controller

The controller of personal data processed in connection with your account on the Werkzeug hosted service at werkzeug.ee (the "Service") is **Werkstatt OÜ**, registry code 14937087, Hansu tn 30, Haabersti linnaosa, Tallinn, Harju maakond, Estonia. Contact: contact@werkzeug.ee.

Where you use the Service to process personal data contained in your company's accounting data, you (or your company) are the controller of that data and we act as your processor under the [Data Processing Agreement](#). This Policy covers the data for which we are the controller.

2. What we collect and store

- **Account data** — your email address and a salted password hash (argon2id). We never store your password in plaintext.
- **Accounting API credentials** — RIK e-Financials API key fields, Erply Books API tokens, and Merit Aktiva API ID and API key you add are stored with AES-256-GCM envelope encryption. Plaintext credential values are never written to the database.
- **MCP API keys** — stored only as keyed hashes (HMAC-SHA256). The plaintext key is shown to you once at creation and cannot be recovered by us.
- **Usage logs** — for each MCP tool call we record the tool name, timestamp, outcome, duration, and the client user-agent string, linked to your account.
- **Billing data** — for paid plans we store Stripe customer and subscription identifiers and subscription status. Your payment card details are held by Stripe, not by us.
- **Password reset tokens** — short-lived hashed tokens valid for one hour.
- **OAuth grants** — where you authorise an MCP client via OAuth, we store client registrations and hashed authorisation codes and tokens linked to your account.
- **Correspondence** — emails you send to our contact addresses.
- **Product feedback** — when you submit feedback or a bug report from the dashboard, we send your message together with your account email, user id, plan, the page URL, and browser user-agent to our feedback inbox (Baserow).

3. What we do not store

Accounting payloads — invoices, journal entries, reports, and other data returned by or sent to a connected accounting API (RIK e-Financials, Erply Books, or Merit Aktiva) — pass through the Service in transit only. They are not persisted in our database.

4. Purposes and legal bases

PURPOSE	DATA	LEGAL BASIS (GDPR)
Providing your account and signing you in	Email, password hash	Contract, Art. 6(1)(b)
Proxying API calls you initiate	Encrypted provider credentials, MCP key hashes, OAuth grants	Contract, Art. 6(1)(b)
Billing for paid plans	Stripe identifiers, subscription status	Contract, Art. 6(1)(b)
Usage metering, dashboards, abuse prevention	Usage logs	Contract and legitimate interests, Art. 6(1)(b) and (f)
Password reset emails	Email, hashed reset token	Contract, Art. 6(1)(b)
Product feedback and bug reports	Message, email, user id, plan, page URL, user-agent	Legitimate interests, Art. 6(1)(f)
Security, incident response, legal compliance	Account data, usage logs, application logs	Legitimate interests, Art. 6(1)(f); legal obligation, Art. 6(1)(c)

We do not use your data for marketing profiling or advertising.

5. Recipients and sub-processors

PROVIDER	ROLE	LOCATION
Hetzner Cloud	Application and database hosting	Helsinki, Finland (EU)
Stripe	Payment processing for paid plans	United States — transfers safeguarded by Standard Contractual Clauses under the Stripe DPA
Resend	Transactional email (password reset)	See Resend's data processing terms

PROVIDER	ROLE	LOCATION
Baserow	Feedback / bug report inbox when that feature is enabled	See Baserow's data processing terms

RIK e-Financials, Erply Books, and Merit Aktiva (Merit Tarkvara AS) are not our sub-processors: API calls are made with your own credentials under your own relationship with each provider. We may also disclose data where required by law or to protect our legal rights.

6. Retention

- Account data, credentials, MCP keys, and OAuth grants are kept for as long as your account exists and are deleted with it.
- Usage log rows are retained after account deletion with the link to your account removed, so they can no longer be attributed to you.
- Password reset tokens expire after one hour and become unusable once used.
- Billing records are retained as long as required by Estonian accounting and tax law (generally seven years).
- Encrypted database backups are kept on a rolling schedule; deleted data leaves the backup window as backups rotate.

7. Security

All traffic uses TLS. Provider credentials are envelope-encrypted with AES-256-GCM; passwords are hashed with argon2id; MCP keys and OAuth tokens are stored only as hashes. Production runs on Hetzner Cloud in the EU. More detail is on the [Security page](#).

8. Your rights

Under the GDPR you have the right to access, rectify, and erase your personal data, to restrict or object to its processing, and to data portability. To exercise these rights, or to delete your account, email contact@werkzeug.ee from the address on your account. We respond within one month.

You also have the right to lodge a complaint with the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon, www.aki.ee) or with the supervisory authority of your place of residence.

9. Cookies and local storage

We do not use tracking cookies or third-party analytics. The Service uses browser storage for functional purposes only: your language preference is kept in `localStorage`, and your dashboard session token is kept in `sessionStorage` and cleared when the tab closes.

10. Changes to this Policy

We will update this Policy when our processing changes. For material changes we will notify you by email or via the dashboard. The version identifier at the top of this page tells you which version is in force.

11. Contact

Privacy questions and requests: contact@werkzeug.ee.

