Data Processing Agreement

Version 2026-08-31 · Effective 31 August 2026

1. Scope and parties

This Data Processing Agreement ("DPA") is entered into between the customer of the Werkzeug hosted service (the "Customer", acting as controller) and **Werkstatt OÜ**, registry code 14937087, Hansu tn 30, Haabersti linnaosa, Tallinn, Harju maakond, Estonia (the "Processor"). It supplements the Terms of Service and is incorporated into them by reference.

This DPA applies where the Customer uses the Service to process personal data contained in accounting data that transits the Service to and from connected accounting APIs (RIK e-Financials and, on eligible plans, Erply Books and Merit Aktiva), within the meaning of Article 28 of Regulation (EU) 2016/679 ("GDPR"). It applies automatically to all plans; for Custom plan customers a countersigned copy is provided as part of onboarding, and Pro customers may request a countersigned copy at contact@werkzeug.ee.

Personal data relating to the Customer's own account (email, billing, usage logs) is processed by Werkstatt OÜ as controller and is covered by the Privacy Policy, not by this DPA.

2. Details of the processing

SUBJECT MATTER	Proxying of API requests between the Customer's MCP clients and connected accounting APIs (RIK e-Financials and, on eligible plans, Erply Books and Merit Aktiva).
DURATION	The term of the Customer's use of the Service under the Terms of Service.
NATURE AND PURPOSE	Transmission only: signing, forwarding, and returning API requests and responses initiated by the Customer. Accounting payload data is processed in transit and not stored.
CATEGORIES OF PERSONAL DATA	Personal data appearing in accounting records, such as names and contact details of the Customer's own customers, suppliers, and employees; invoice lines; payment references; bank details contained in accounting entries.
CATEGORIES OF DATA SUBJECTS	The Customer's customers, suppliers, employees, and other natural persons appearing in the Customer's accounting records.
SPECIAL CATEGORIES OF DATA	None intended. The Customer must not use the Service to process special categories of personal data (Art. 9 GDPR).

3. Instructions

The Processor processes personal data only on the Customer's documented instructions, including with regard to transfers to third countries, unless required to do otherwise by EU or member state law; in that case the Processor informs the Customer before processing, unless the law prohibits it. The Customer's instructions are: to transmit API requests and responses between the Customer's MCP clients and the connected accounting API the Customer has configured (RIK e-Financials, Erply Books, or Merit Aktiva) as initiated through the Service. The Processor will inform the Customer if, in its opinion, an instruction infringes the GDPR.

4. Confidentiality

The Processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Security measures (Art. 32 GDPR)

- All traffic in transit is protected with TLS; upstream requests are authenticated with the Customer's provider credentials (RIK e-Financials uses HMAC-SHA384; Erply Books and Merit Aktiva use each provider's own signing scheme).
- Customer API credentials are stored with AES-256-GCM envelope encryption; plaintext is never persisted.
- MCP API keys and OAuth tokens are stored only as keyed hashes.
- Accounting payload data is not persisted; it is processed in memory for the duration of each request.
- Production infrastructure is hosted in the EU (Hetzner Cloud, Helsinki) with access restricted to authorised personnel.
- The server core is open source and publicly auditable.

Further detail is published on the Security page. The Processor may update these measures provided the overall level of security is not reduced.

6. Sub-processors

The Customer grants a general authorisation for the engagement of sub-processors. The Processor imposes on each sub-processor data protection obligations equivalent to those in this DPA and remains liable for their performance. Sub-processors currently engaged for the processing under this DPA:

SUB-PROCESSOR	PURPOSE	LOCATION
Hetzner Cloud	Hosting of the application infrastructure through which accounting data transits	Helsinki, Finland (EU)

RIK e-Financials, Erply Books, and Merit Aktiva (Merit Tarkvara AS) are not sub-processors: the Customer maintains its own direct relationship with each provider, and API calls are made with the Customer's own credentials. Stripe and Resend process only account and billing data covered by the Privacy Policy, not accounting data under this DPA.

The Processor will give at least 30 days' notice of intended additions or replacements of sub-processors (by email or via the dashboard). The Customer may object on reasonable data protection grounds; if no solution is found, the Customer may terminate the affected Service.

7. Assistance to the Customer

Taking into account the nature of the processing — transit-only, with no storage of accounting data — the Processor assists the Customer with appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Customer's obligations to respond to data subject requests (Arts. 12–23 GDPR) and in ensuring compliance with Arts. 32–36 GDPR (security, breach notification, data protection impact assessments, and prior consultation). Because accounting data is not stored by the Processor, data subject requests concerning it are normally fulfilled by the Customer directly in the connected accounting system.

8. Personal data breach

The Processor notifies the Customer without undue delay after becoming aware of a personal data breach affecting personal data processed under this DPA, and provides the information reasonably required for the Customer to meet its own notification obligations under Arts. 33 and 34 GDPR.

9. Deletion and return

Accounting data is not stored by the Processor, so there is nothing to return at the end of the Service. Upon termination of the Service, the Processor deletes the Customer's stored account data, including encrypted provider credentials and MCP keys, as described in the Privacy Policy, unless EU or member state law requires further storage.

10. Audits and information

The Processor makes available to the Customer the information necessary to demonstrate compliance with Article 28 GDPR, including the published security documentation and the open-source code base, and allows for and contributes to audits conducted by the Customer or an auditor mandated by the Customer, subject to reasonable notice, at most once per year, during business hours, and without disrupting the Service. The Customer bears the costs of audits it initiates.

11. International transfers

Personal data processed under this DPA is processed within the European Union. The Processor will not transfer it outside the EU/EEA without ensuring a valid transfer mechanism under Chapter V GDPR and notifying the Customer under Section 6.

12. Liability, term, and precedence

The liability provisions of the Terms of Service apply to this DPA. This DPA takes effect when the Customer starts using the Service and remains in force for as long as the Processor processes personal data under it. In case of conflict between this DPA and the Terms of Service regarding the processing of personal data, this DPA prevails. This DPA is governed by the laws of the Republic of Estonia.

13. Contact

Data processing questions and countersigned copies: contact@werkzeug.ee.