

Data Processing Agreement (DPA)

pursuant to Art. 28 GDPR – Auftragsverarbeitungsvertrag

1. Parties and Scope

This Data Processing Agreement ("DPA") forms part of the agreement between the customer ("Controller") and TECHARENABG EOOD ("Processor", "we", "InboxDoc"), and governs the processing of personal data by the Processor on behalf of the Controller in connection with the InboxDoc invoice-processing service.

2. Subject Matter and Duration

The subject matter of this DPA is the processing of personal data carried out by the Processor on behalf of the Controller in order to provide the InboxDoc service: scanning the Controller's connected email accounts for invoice-bearing messages, extracting structured invoice data, and making that data available in the Controller's dashboard.

This DPA remains in effect for as long as the Processor processes personal data on the Controller's behalf, and terminates automatically when the underlying service agreement ends and all personal data has been deleted or returned in accordance with Section 12.

3. Nature and Purpose of Processing

The Processor processes personal data exclusively to: connect to the Controller's nominated email accounts (Gmail, Outlook, or IMAP) via the access the Controller has granted; identify email messages that contain, or are likely to contain, invoice or credit-note attachments; extract structured invoice fields from those attachments (deterministically from structured e-invoice XML where available, or via AI-assisted extraction from the PDF otherwise); and store, display, and export the extracted structured data via the Controller's dashboard.

4. Categories of Personal Data

- Account data of the Controller's users (name, email address)
- Email metadata of scanned messages (sender, subject line, date)
- Data extracted from invoices/credit notes (vendor name, invoice number, dates, amounts, currency) – this may incidentally include personal data where an invoice names a natural person as vendor or customer
- OAuth access/refresh tokens, or an encrypted IMAP app password, used solely to maintain the email connection
- Approximate country, derived once from the IP address at signup; the IP address itself is not retained

5. Categories of Data Subjects

The Controller's own account users (e.g. employees with dashboard access), and third parties named on invoices processed through the service (e.g. vendor contacts, individual sole traders invoicing the Controller).

6. Controller's Rights and Obligations

The Controller remains solely responsible for the lawfulness of the personal data it submits for processing (including the email accounts it connects) and for responding to data subject requests, except to the extent the Processor is required to assist under Section 10. The Controller is responsible for issuing documented instructions to the Processor; this DPA, together with the Controller's ordinary use of the Service's documented features, constitutes such instructions.

7. Processor's Obligations

- The Processor shall process personal data only on documented instructions from the Controller, including with regard to international transfers, unless required to do otherwise by EU or member state law.
- The Processor ensures that persons authorised to process personal data have committed themselves to

confidentiality.

- The Processor shall not retain source files (PDF attachments or e-invoice XML files) – only the structured data fields extracted from them are stored.
- The Processor shall implement the technical and organisational measures described in Section 8.
- The Processor shall not engage another processor (sub-processor) without the Controller's prior general authorisation, which the Controller grants hereby for the sub-processors listed in Section 9; the Processor will inform the Controller of any intended changes concerning the addition or replacement of sub-processors, giving the Controller the opportunity to object.

8. Technical and Organisational Measures (TOMs)

- Encryption of OAuth tokens and IMAP app passwords at rest; HTTPS/TLS for all data in transit
- Row-level security in the database, so each customer's data is only accessible to that customer's own account
- No retention of source PDF/XML files – only extracted structured fields are stored (see Privacy Policy)
- Least-privilege OAuth scopes for Gmail/Outlook access; no passwords are ever requested or stored for Gmail/Outlook (IMAP app passwords are encrypted, never stored in plain text)
- Multi-factor authentication (MFA) available for account access
- Access control: internal access to production data is limited to personnel who need it for support/operations
- Deterministic, non-AI extraction is used wherever possible (structured e-invoice XML); AI-assisted extraction is used only as a fallback, and only on the document itself, never on account credentials

9. Sub-processors

The Controller authorises the Processor to engage the following sub-processors:

- Supabase – database hosting, authentication – EU (Ireland, eu-west-1)
- Vercel Inc. – application hosting / serverless functions – EU (Dublin, dub1; pinned)
- Cloudflare, Inc. – network-level proxy / DNS
- Anthropic, PBC – AI-assisted invoice data extraction (fallback path only; not used for e-invoices processed via structured XML) – USA; transfer safeguard: Standard Contractual Clauses (Art. 46 GDPR)
- Lemon Squeezy, Inc. (a Stripe company) – payment processing, acting as merchant of record
- Google LLC – Gmail API access (with the Controller's explicit consent); Google Analytics (GA4), only after cookie consent – USA
- Microsoft Corporation – Outlook / Microsoft Graph API access (with the Controller's explicit consent)

10. Assistance with Data Subject Requests

Taking into account the nature of the processing, the Processor shall assist the Controller, insofar as reasonably possible, in fulfilling the Controller's obligation to respond to requests from data subjects exercising their rights under Chapter III GDPR. Where a data subject contacts the Processor directly, the Processor will redirect the request to the Controller without undue delay, unless instructed otherwise.

11. Personal Data Breach Notification

The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach affecting the Controller's data, and shall provide reasonable assistance with the Controller's own notification obligations under Art. 33/34 GDPR.

12. Deletion or Return of Data on Termination

Upon termination of the underlying service agreement, the Processor shall, at the Controller's choice, delete or return all personal data processed on the Controller's behalf, and delete existing copies, unless EU or member state law requires continued storage. Account deletion initiated by the Controller through the Service's self-service "Delete account" feature immediately and irreversibly deletes extracted invoice data, revokes OAuth tokens with the provider, and deletes profile and notification data, as described in the Privacy Policy.

13. Audits

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations in this DPA and Art. 28 GDPR, and shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, subject to reasonable advance notice and confidentiality.

14. Liability

Liability between the parties in connection with this DPA is governed by the liability provisions of the underlying Terms of Service.

15. Governing Law

This DPA is governed by the laws of Bulgaria and the General Data Protection Regulation (EU) 2016/679.

TODO(legal-review): This entire document is a drafted template reflecting the technical setup described to us; it has not been reviewed by a data protection lawyer and should not be relied upon, signed, or sent to customers as a binding legal document before that review.