Data Processing Agreement (DPA)

pursuant to Art. 28 GDPR

BiGapi File Processing API (api.bigapi.dev)

> **Contracting Parties:** This Data Processing Agreement is entered into between the customer using the Service under the Terms of Service (**"Controller"**) and **Artoption GmbH**, Am Wiesenrain 14, 71720 Oberstenfeld, Germany (**"Processor"**), together the **"Parties"**.

1. Subject matter and duration

1.1 The Processor provides file-processing operations via the API at `api.bigapi.dev` (the "Service"), as described in the Terms of Service. In doing so, the Processor may process personal data contained in files the Controller submits, on behalf of the Controller.

1.2 This DPA applies for as long as the Controller uses the Service and forms part of the contract under the Terms of Service. It is concluded by the Controller's use of the Service for the processing of personal data; a signed copy is available on request.

2. Nature and purpose of processing, data and data subjects

2.1 Nature and purpose: technical, automated processing of files submitted by the Controller (e.g. rendering to PDF/PNG, PDF manipulation, OCR, format conversion, image processing) for the sole purpose of returning the requested result to the Controller. The Processor has no knowledge of, and does not evaluate, the content of files.

2.2 Types of personal data: any personal data the Controller chooses to include in submitted files (e.g. names, contact details, contract or invoice data, identifiers). The Processor does not require or request any specific data. Special categories of data (Art. 9 GDPR) may be contained in files at the Controller's discretion; the Controller is responsible for the lawfulness of such processing.

2.3 Categories of data subjects: persons whose data is contained in the Controller's files (e.g. the Controller's customers, employees, business contacts).

2.4 Not covered by this DPA: account and billing data of the Controller itself (API key hashes, email address, balance, usage metadata) – processed by the Processor as an independent controller under the Privacy Policy; and payment data processed by Stripe as merchant of record under Stripe's own terms.

3. Obligations of the Processor (Art. 28(3) GDPR)

The Processor shall:

- **a)** process personal data only on documented instructions from the Controller. The instruction consists of the API request itself (operation and parameters); the Processor performs no processing beyond the requested operation. If the Processor is required by EU or Member State law to process otherwise, it will inform the Controller before processing unless prohibited by law;
- **b)** ensure that persons authorised to process the data are bound by confidentiality. In normal operation, no natural person accesses submitted files; processing is fully automated;
- **c)** implement the technical and organisational measures set out in Annex 2;
- **d)** engage sub-processors only as listed in Annex 1 and under the conditions of Section 5;
- **e)** taking into account the nature of the processing, assist the Controller in responding to data-subject requests – noting that, due to the design of the Service (no retention of files, see Annex 2), the Processor holds no personal data from files after delivery of the result and therefore cannot rectify, restrict, or export such data;

- **f)** assist the Controller in ensuring compliance with Art. 32–36 GDPR, taking into account the nature of the processing and the information available to the Processor;
- **g)** delete all personal data contained in submitted files immediately upon delivery of the result (see Annex 2); no copies are retained. Log and usage records contain no file content, file names, or personal data from files;
- **h)** make available all information necessary to demonstrate compliance with Art. 28 GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller (Section 6).

4. Personal data breach

The Processor shall notify the Controller without undue delay, and no later than 48 hours after becoming aware, of a personal data breach affecting the Controller's data, with the information required by Art. 33(3) GDPR to the extent available. Notification is made to the email address associated with the Controller's account.

5. Sub-processors

5.1 The Controller authorises the sub-processors listed in Annex 1.

5.2 The Processor will inform the Controller of any intended addition or replacement of sub-processors by publishing an updated Annex 1 at the Service website with at least 30 days' notice. The Controller may object on reasonable data-protection grounds within that period; if no solution is found, the Controller may terminate the use of the Service. Continued use after the notice period constitutes acceptance.

5.3 The Processor imposes on each sub-processor data-protection obligations that are essentially equivalent to those in this DPA.

6. Audits

The Controller may verify compliance with this DPA once per year, or after a personal data breach, by requesting the information described in Annex 2 and, where reasonably required, by an on-site or remote inspection at the Controller's expense, with reasonable notice and without disrupting the Service. The Processor may satisfy audit requests by providing current documentation and, where available, third-party certifications of its sub-processors.

7. International transfers

Processing of files takes place exclusively on servers in Germany (Hetzner Online GmbH, Falkenstein). Account metadata is stored in the EU (Supabase, region Frankfurt). Payment processing by Stripe, Inc. as merchant of record may involve transfers to the USA on the basis of the EU-US Data Privacy Framework and/or Standard Contractual Clauses; these transfers concern the Controller's payment data, not files.

8. Deletion and return

Because files are deleted immediately after delivery of each result (Annex 2), no return or deletion at the end of the contract is required for file contents. Usage and billing records are retained as required by tax and commercial law (§ 147 AO, § 257 HGB).

9. Liability and final provisions

Liability follows the Terms of Service. German law applies; if the Controller is a merchant, the exclusive place of jurisdiction is Stuttgart, Germany. Should provisions of this DPA conflict with the Terms of Service, this DPA prevails with respect to the processing of personal data on behalf of the Controller.

Annex 1 – Sub-processors

Sub-processor	Purpose	Location	Basis
Hetzner Online GmbH Gunzenhausen (DE)	Hosting of processing servers (API gateway and processing engine)	Falkenstein, Germany	DPA with Hetzner (Art. 28)
Supabase, Inc.	Database for account metadata (key hashes, balances, usage metadata) – no file contents	EU (Frankfurt)	DPA with Supabase; SCCs where applicable
Stripe, Inc. / **Stripe Payments Europe Ltd.**	Payment processing and invoicing as merchant of record – acts as independent controller for payment data	EU / USA	Stripe terms; EU-US DPF / SCCs

Annex 2 – Technical and organisational measures (Art. 32 GDPR)

A. Data minimisation by design

- Files are processed exclusively in volatile memory (RAM-based temporary file system, 2 GB tmpfs) on the processing server; they never touch persistent disk storage.
- Each request runs in an isolated temporary working directory that is created for the request and deleted recursively upon completion of the request, regardless of success or failure. Intermediate files (e.g. OCR conversions) are deleted as well.
- Neither the gateway nor the processing engine mounts persistent volumes; there are no backups or snapshots containing customer files.
- The service is stateless with respect to files: nothing is cached or stored between requests.

B. Logging and retention

- Application logs (gateway, engine) record only request method, URL path, HTTP status, and response time – no request bodies, no file names, no file contents.
- The reverse proxy access log removes the Authorization, X-Ops-Token, and Cookie headers before writing and masks client IP addresses (IPv4 /24, IPv6 /48). Access logs are rotated (50 MB, max. 3 files) and retained for a maximum of 7 days.
- Container logs are limited to 3 × 10 MB per service (rolling).
- Usage records (for billing) contain operation type, cost, HTTP status, duration, page count, output size, and an optional customer-chosen idempotency key – no file content or file names.

C. Access control and credentials

- Customer API keys are stored only as SHA-256 hashes; the plaintext key is shown once at creation and cannot be recovered by the Processor.
- Administrative interfaces are protected by a separate token and HTTP authentication; SSH access to servers is key-based, root login disabled, intrusion protection (fail2ban) active.
- Secrets (database, payment provider) are held in server-side environment configuration only and rotated on suspicion of exposure.

D. Transport and infrastructure security

- All API traffic is encrypted in transit (TLS 1.3, automatic certificate management); HTTP is redirected to HTTPS.
- The processing engine is reachable only from the internal container network, not from the internet.
- Host firewall restricts inbound traffic to ports 22/80/443; operating-system security updates are applied regularly.
- Servers are located in Germany (Falkenstein); the database region is Frankfurt (EU).

E. Availability and monitoring

- Automated self-test of all operations twice daily with alerting in the operations dashboard; container restart policies; daily infrastructure backups of the host (system configuration – not customer files, which are never stored).

F. Organisational measures

- Processing is fully automated; no staff member accesses customer files in normal operation.
- Changes to the processing pipeline are versioned and deployed with a documented procedure; this Annex is reviewed after each relevant change.