Agreement according to Art. 28 GDPR

Between

_____
(Company name and person of contact)

_____
(Street)

_____
(ZIP and City)

_____
(Country)

- hereinafter referred to as the controller –

And

QaamGo Web GmbH
Fritz-Reichle-Ring 2
78315 Radolfzell
Germany

- hereinafter referred to as the processor -

1. Subject matter and duration of the contract

(1) Subject matter of the contract
The subject matter of the contract is for the processor to carry out the following tasks: Conversion and editing of e-book and other document and image files.
(2) Duration
This contract is concluded for an indefinite period and is terminated at the moment that the agreement governing the supply of the service defined in Article 2 by the processor (the underlying agreement) is terminated according to Paragraph 5 of the Terms and Conditions of Processor (the underlying agreement). This contract cannot be terminated independently of the underlying agreement, except by superseding this contract with another contract governing the same subject matter.

2. Contract details

(1) Nature and purpose of processing of personal data
Detailed description of the subject matter of the contract with regard to the nature and purpose of the services provided by the processor: Usage of the web service of https://www.ebook2edit.com/.

In principle, the undertaking of the agreed processing of data shall be carried out in a member state of the European Union (EU) or another contracting state of the European Economic Area (EEA). Any transfer to a third country requires the prior consent of the controller and may only take place if the specific requirements of Article 44 et seq. GDPR have been satisfied.

(2) Type of data

The subject matter of the processing of personal data includes the following types/ categories of data (list/ description of the data categories)

- Personal master data
- Communication data (e.g. telephone, email)
- Contract master data (contractual relationship, contractual or product interest)
- Contract billing and payment data
- Planning and control data
- IP-Data

(3) Categories of data subjects

The categories of data subjects include:

- Customers of controller
- Prospective customers of controller
- Employees of controller
- Suppliers

(4) Scope of data processing:

Collect, store, modify, transmit, block, delete and use the data for the respective purposes

(5) Purpose of data processing:

The purpose of the data processing is the use of the service provided by the contractor in accordance with his general terms and conditions at https://www.ebook2edit.com/

3. Technical and organisational measures

(1) Before the commencement of processing, the processor shall document the execution of the necessary technical and organisational measures, set out in advance of the awarding of the order or contract, specifically with regard to the detailed execution of the contract, and shall present these to the controller for review. Upon acceptance by the controller, the documented measures become the foundation of the contract. If the measures need to be adjusted following the review/audit by the controller, this shall be implemented with the agreement of both parties.

(2) The processor shall ensure an appropriate level of security in accordance with Article 28 (3) (c) and Article 32 GDPR, in particular in conjunction with Article 5 (1) and (2) GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. At the same time, the measures shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the varying likelihood and severity of risks for the rights and freedoms of natural persons in accordance with Article 32 (1) GDPR [for details, please refer to Annex 1].

(3) The technical and organisational measures shall be adapted to reflect technical progress and further developments. In this respect, the processor is permitted to implement alternative adequate

measures. In so doing, the security level of the defined measures may not be reduced. Any significant changes shall be documented.

4. Rectification, blocking and erasure of data

(1) The processor may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the controller, but only on documented instructions from the controller. If the data subject contacts the processor directly concerning a rectification, erasure, or restriction of processing, the processor shall promptly forward the data subject's request to the controller.
(2) Where this is included within the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the processor in accordance with documented instructions from the controller without undue delay.

5. Quality assurance and other obligations of the processor

In addition to complying with the provisions of this contract, the processor is required to satisfy the requirements under Articles 28 to 33 GDPR; the processor shall ensure, in particular, compliance with the following requirements:

- **a)** The processor is not obliged to designate a data protection officer. Jens Bierkandt, Telephone: +49 7732/9391656, e-mail: j.bierkandt@qaamgo.com] has been designated as a contact person for the processor.
- **b)** Confidentiality obligation in accordance with Article 28 (3) (2) (b), Article 29 and Article 32 (4) GDPR. The processor shall only entrust such employees with the implementation of the contract who have committed themselves to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The processor and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the controller, which includes the powers granted in this contract, unless required to do so by law.
- **c)** The processor shall implement and comply with all technical and organisational measures necessary for this contract pursuant to Articles 28 (3) (2) (c) and 32 GDPR [for details, please refer to Annex 1].
- **d)** The controller and the processor shall cooperate, on request, with the supervisory authority in the performance of their tasks.
- **e)** The processor shall promptly notify the controller of any inspections and measures taken by the supervisory authority, insofar as they relate to this contract. This also applies where the processor is under investigation or is party to an investigation by a competent authority in connection with infringements to any civil or criminal law, or administrative rule or regulation regarding the processing of personal data in connection with the processing of this contract.
- **f)** The processor shall endeavour to support the controller where the controller is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a data subject or by a third party or any other claim in connection with data processing by the processor.
- **g)** The processor shall periodically monitor the internal processes and the technical and organisational measures to ensure that processing within its area of responsibility is in accordance with the requirements of applicable data protection laws and regulations and the protection of the rights of the data subject.

h) Verifiability of the implemented technical and organisational measures in relation to the controller within the scope of the controller's control powers under Section 7 of this contract.

6. Subprocessing

(1) For the purposes of this provision, subprocessors provide services that directly relate to the provision of the main service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The processor shall, however, conclude adequate data processing agreements for third-party ancillary services that comply with the relevant laws and take control measures to ensure the confidentiality and security of personal data of the controller.

(2) The processor may only engage subprocessors (other processors) after prior express written consent from the controller.

a) The controller agrees to the engagement of the following subprocessors based on a contract in accordance with Articles 28 (2) to (4) GDPR:

Company subprocessor	Address/ country	Service
Hetzner Online GmbH	Gunzenhausen/Germany	Hosting

b)

Changes of the existing subprocessor
are permitted if:

- the processor notifies the controller of such outsourcing to a subprocessor in advance in writing or in electronic form and
- the controller has not objected to the planned outsourcing in writing or in electronic form by the time the data is handed over to the processor and
- this is based on a contract in accordance with Articles 28 (2) to (4) GDPR.

(3) The transfer of personal data of the controller to the subprocessor and the commencement of the subprocessor's initial activities are only permitted if all requirements for subcontracting have been met.
(4) If the subprocessor provides the agreed service outside the EU/EEA, the processor shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies where service providers within the meaning of Section 1 sentence 2 should be used.
(5) Further outsourcing by subprocessors requires the express consent of the main processor (at least in electronic form);

All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subprocessor.

7. Supervisory rights of the controller

(1) The controller is entitled to exercise processing control or to have processing monitored by an auditor to be appointed on a case-by-case basis. The controller has the right to satisfy itself through

random checks, which, as a rule, must be notified in good time, of the processor's compliance with this agreement.
(2) The processor shall ensure that the controller can satisfy itself of the compliance with the obligations of the processor in accordance with Article 28 GDPR. The processor undertakes to give the controller the necessary information on request and, in particular, to demonstrate the execution of the technical and organisational measures.
(3) The proof of such measures, which do not concern only the concrete contract, may be provided by

- ✓ compliance with an approved code of conduct in accordance with Article 40 GDPR;
- ✓ certification according to an approved certification procedure in accordance with Article 42 GDPR;
- ✓ current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, data protection officer, IT security department, data privacy auditor, quality auditor);
- ✓ a suitable certification through IT security or data protection audit (e.g. in accordance with BSI-Grundschutz, i.e. IT baseline protection certification developed by the German Federal Office for Security in Information Technology (BSI)).

(4) The processor may assert a claim for reimbursement of reasonable expenses in order to allow checks by the controller.

8. Notification in the case of non-compliance by the processor

(1) The processor shall assist the controller in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations in accordance with Articles 32 to 36 GDPR. This includes but is not limited to:

a) Ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events
b) The obligation to report a personal data breach promptly, whithin 48 hours at the latest to the controller
c) The duty to assist the controller with regard to the controller's obligation to provide information to the data subject concerned and to immediately provide the controller with all necessary information in this regard
d) Supporting the controller with its data protection impact assessment
e) Supporting the controller with regard to prior consultation of the supervisory authority

(2) The processor may claim compensation for support services, which are not included in the description of the services and which are not attributable to failures on the part of the processor.

9. Controller's authority to issue instructions

(1) The controller shall immediately confirm oral instructions (at least in electronic form).
(2) The processor shall inform the controller immediately if he considers that an instruction violates data protection regulations. The processor shall then be entitled to suspend the execution of the relevant instructions until the controller confirms or changes them.

10. Erasure and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the controller. This does not apply to back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.
(2) Upon completion of the contractually agreed work, or earlier if requested by the controller - but no later than by the end of the contractual relationship - the processor shall hand over to the controller any documents that came into its possession, as well as any results derived from the processing and use of data, including any data resources related to the contract or destroy the data with the prior consent of the controller in compliance with data protection regulations. The same shall apply to test and reject material. A record of the deletion shall be provided upon request.
(3) Any documentation that serves the purpose of providing proof of proper data processing shall be kept by the processor for the respective retention periods, even if they extend beyond the term of the contract. The processor can hand over the documentation upon termination of the agreement with discharging effect.

_____

Date and Signatures controller Date and Signatur processor

Please send two copies of this document signed to the processor. Processor will sign it and send back one copy to the controller.

Annex - Technical and organisational measures

1. Confidentiality (Article 32 (1) (b) GDPR)
    - Physical access control
      No unauthorised access to data processing facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV systems;
    - Equipment access control
      No unauthorised system usage, e.g. (secure) passwords, automatic locking mechanisms, two-factor authentication, encryption of data carriers;
    - Data access control
      No unauthorised reading, copying, modification or removal within the system, e.g. authorisation policy and needs-based access rights, logging of access;
    - Separability
      Separate processing of data collected for different purposes, e.g. multi-client capability, sandboxing;
    - Pseudonymisation (Article 32 (1) (a) GDPR; Article 25 (1) GDPR)
      The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures;

2. Integrity (Article 32 (1) (b) GDPR)

- Data transfer control
  No unauthorised reading, copying, modification or removal during electronic transmission or transport, e.g.: encryption, virtual private networks (VPN), electronic signatures;
- Input control
  Verification, whether and by whom personal data is entered into a data processing system, is changed or deleted, e.g. logging, document management;

3. Availability and resilience (Article 32 (1) (b) GDPR)

- Availability control
  Protection against accidental or wilful destruction or loss, e.g. backup strategy (online/offline, on-site/off-site), uninterruptible power supply (UPS), antivirus, firewall, reporting and contingency plans;
- Ability to restore the availability and access in a timely manner (Article 32 (1) (c) GDPR);

4. Process for regularly testing, assessing and evaluating (Article 32 (1) (d) GDPR; Article 25 (1) GDPR)

- Data protection management;
- Incident response management;
- Data protection by default (Article 25 (2) GDPR);
- Processing control
  Data processing within the meaning of Article 28 GDPR can only take place on instructions from the controller, e.g.: clear contract design, formalised order management, strict selection of service providers, duty of pre-evaluation, supervisory follow-up checks.