Data Processing Agreement pursuant to Art. 28 GDPR

Version 1.0 · Last updated: 18 May 2026

This online version shows the DPA with placeholders ([Customer Company] etc.). The actual contract data is filled in offline at contract signing.

As of: [Date]

Preamble

Between

[Customer Company Name]
[Address]
[Postal Code, City]

— hereinafter "Controller" —

and

AGC Consult
Friedenstraße 59
97072 Würzburg, Germany

— hereinafter "Processor" —

§ 1 Subject and Duration of Processing

(1) The subject of this Agreement is the processing of personal data by the Processor on behalf of the Controller within the scope of providing the Software-as-a-Service solution "AGC Suite" and related services (implementation, support, consulting).

(2) The Agreement applies for the duration of the underlying main contract between the parties.

(3) Upon termination of the main contract, this Data Processing Agreement also ends, subject to the provisions on data deletion and retention pursuant to § 10.

§ 2 Nature and Purpose of Processing

(1) Processing takes place for the purpose of providing and operating AGC Suite and rendering related services for the Controller.

(2) The nature of processing includes in particular: collecting, recording, organizing, structuring, storing, adapting, retrieving, querying, using, transmitting (within the recipients authorized by the Controller), aligning, combining, restricting, erasing or destroying personal data.

§ 3 Nature of Personal Data

The following categories of personal data may be processed within the scope of this Agreement:

- Master data (e.g. name, address, date of birth, gender)
- Contact data (e.g. telephone, e-mail, business addresses)
- Contract data (e.g. contractual relationships, conditions, terms)
- Communication data (e.g. correspondence, conversation notes)
- Identification data (e.g. ID document information in the context of KYC processes, where processed by the Controller)
- Sales and transaction data (e.g. offers, orders, revenues)
- IT usage data (e.g. login times, IP addresses, activity logs of AGC Suite users)

§ 4 Categories of Data Subjects

Data subjects may include:

- Employees and users of AGC Suite at the Controller's organization
- Customers, prospects and business partners of the Controller
- Contractual partners of the Controller
- Other persons whose data the Controller processes in AGC Suite in the course of its business activity

§ 5 Obligations of the Processor

(1) The Processor processes personal data exclusively on documented instructions from the Controller. This also applies to the transfer of personal data to a third country or an international organization, unless required to do so by Union or Member State law.

(2) The Processor informs the Controller immediately if it considers that an instruction violates applicable data protection law.

(3) The Processor ensures that persons authorized to process personal data have committed themselves to confidentiality or are subject to an appropriate statutory obligation of confidentiality.

(4) The Processor supports the Controller, to the extent possible, in fulfilling requests and claims of data subjects pursuant to Chapter III of the GDPR and in complying with the obligations set out in Articles 32 to 36 GDPR.

(5) The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and allows for audits pursuant to § 9 of this Agreement.

§ 6 Obligations of the Controller

(1) Within the scope of the contractual relationship, the Controller is responsible for compliance with statutory data protection provisions, in particular for the lawfulness of the transfer of data to the Processor and for the lawfulness of data processing.

(2) The Controller issues instructions in writing or in a documented electronic format. Verbal instructions must be confirmed in writing or electronically without undue delay.

(3) The Controller informs the Processor immediately if it identifies errors or irregularities in the processing.

§ 7 Technical and Organizational Measures (TOMs)

(1) The Processor implements the necessary technical and organizational measures pursuant to Art. 32 GDPR to ensure the security of processing. The measures are documented in Annex 1 to this Agreement.

(2) The measures are reviewed regularly and adapted to the current state of the art.

(3) Significant changes to the measures are coordinated with the Controller and documented.

§ 8 Sub-Processors

(1) The Controller approves the use of the following sub-processors upon conclusion of this Agreement:

Name	Address	Service	Location of Processing
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Germany	Hosting of AGC Suite	Falkenstein, Germany

(2) The Processor informs the Controller of intended changes regarding the addition or replacement of further sub-processors at least 30 days before the change in text form. The Controller has the right to object to such changes.

(3) In the event of a justified objection by the Controller that cannot be resolved amicably within a reasonable period, the Controller has the right to extraordinary termination of the main contract.

(4) The Processor contractually obliges sub-processors to data protection obligations equivalent to those agreed in this Agreement.

§ 9 Controller's Audit Rights

(1) The Controller has the right to verify compliance with the agreed obligations at the Processor. Upon request, the Processor provides appropriate evidence (e.g. current TOMs, certifications, audit reports).

(2) On-site audits are possible after prior notification with reasonable notice (at least 14 days) during normal business hours. They must not unreasonably impair the Processor's business operations.

(3) The Processor is entitled to invoice the effort for extensive audits exceeding the usual scope at customary market conditions.

§ 10 Deletion and Return of Data

(1) After termination of the main contract, the Processor makes the personal data available to the Controller for a period of 30 days for export.

(2) After expiry of the export period, the Processor deletes all personal data of the Controller from its systems, including backups, unless statutory retention obligations preclude this.

(3) The deletion is confirmed in writing to the Controller upon request.

(4) Backup data is automatically deleted after 30 days.

§ 11 Notification of Personal Data Breaches

(1) The Processor informs the Controller immediately, at the latest within 24 hours of becoming aware, of personal data breaches as well as of significant disruptions in order processing.

(2) The notification includes, to the extent available at the time of notification:

- Description of the nature of the breach
- Categories and approximate number of data subjects and records concerned
- Likely consequences
- Measures taken or proposed to remedy the breach

(3) The Processor supports the Controller in fulfilling any reporting obligations to supervisory authorities and data subjects pursuant to Art. 33 and 34 GDPR.

§ 12 Liability

The liability of the parties is governed by the general statutory provisions, in particular Art. 82 GDPR, and the provisions of the main contract.

§ 13 Final Provisions

(1) In case of contradictions between this Agreement and provisions from other agreements between the parties — in particular the main contract — the provisions of this Agreement take precedence in matters of data protection.

(2) Should individual provisions of this Agreement be or become invalid, this shall not affect the validity of the remaining provisions.

(3) Amendments and additions to this Agreement require written form.

(4) German law applies. Place of jurisdiction is Würzburg.

Annex 1: Technical and Organizational Measures (TOMs)

The following technical and organizational measures are implemented by the Processor and its hosting sub-processor Hetzner Online GmbH to ensure the security of processing pursuant to Art. 32 GDPR.

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

Physical Access Control (protection against unauthorized physical access):

- Data centers with controlled access, video surveillance, alarm systems (Hetzner)
- Access only for authorized personnel via authentication
- Documented visitor logs

System Access Control (protection against unauthorized system use):

- Authentication via username and password, password policies (minimum length, complexity)

- Multi-factor authentication available
- Automatic lock-out after repeated failed entries
- Encrypted transmission of access credentials (TLS)

Data Access Control (protection against unauthorized access to data):

- Role and authorization concept within AGC Suite
- Differentiated access rights per user role
- Logging of access and changes (audit trail)
- Separation of production and test environments

Separation Control (separate processing of separately collected data):

- Multi-tenant architecture, logical separation of customer data
- Dedicated databases or schemas per tenant

Pseudonymization and Encryption:

- Encrypted data transmission (TLS 1.2 or higher)
- Encrypted storage of sensitive data in the database
- Encrypted backups

2. Integrity (Art. 32 para. 1 lit. b GDPR)

Transfer Control (protection during electronic transmission):

- Encrypted transmission via HTTPS/TLS
- Secure API access with authentication

Input Control (traceability of changes):

- Logging of data entry, modification and deletion
- Audit trail with timestamp and user identification

3. Availability and Resilience (Art. 32 para. 1 lit. b and c GDPR)

- Daily automated backups, retention 30 days
- Redundant infrastructure of the hosting provider (Hetzner)
- Emergency plan for recovery in case of damage
- Monitoring of availability and system status
- Protection against DDoS attacks at infrastructure level (Hetzner)
- Antivirus and malware protection at system level

4. Procedures for Regular Review (Art. 32 para. 1 lit. d GDPR)

- Regular review of the effectiveness of the TOMs

- Timely deployment of security updates and patches
- Training and awareness of personnel involved in processing
- Privacy-friendly default settings (Privacy by Default)
- Data protection by design (Privacy by Design)

5. Order Control (processing in the sense of the Controller)

- Processing exclusively on documented instructions of the Controller
- Written agreement of obligations in this DPA
- Selection of sub-processors according to data protection criteria
- Contractual obligation of sub-processors to equivalent standards

Note: These TOMs reflect the state as of [Date] and are reviewed regularly and adapted to the current state of the art. Significant changes are communicated to the Controller.

Note on language: This English version is provided for convenience only. In case of discrepancies between the German and English version, the German version shall prevail.

> **Note on language:** This English version is provided for convenience only. In case of discrepancies between the German and English version, the German version shall prevail.