

pursuant to Art. 28 GDPR (DSGVO)**Annex to the General Terms and Conditions (GTC / AGB) of BERYK Consulting GmbH**

This Data Processing Agreement ("AVV") is an annex to the General Terms and Conditions of BERYK Consulting GmbH and governs the processing of personal data on behalf of the "Controller" and the "Processor".

Processor is:

BERYK Consulting GmbH, Friedrichstr. 155, 10117 Berlin

As of: 14 October 2026

Controller is the user who, when registering for the quupp service under § 8 GTC, confirms that they are acting as an entrepreneur within the meaning of § 14 BGB and accepts the GTC in doing so. With this registration and acceptance of the GTC, this AVV automatically becomes part of the main contract between the parties regarding use of the quupp service (§ 8(3) GTC) without separate signing.

1 Subject matter and term

1.1 In the context of the main contract, the Processor processes personal data for which the Controller is responsible within the meaning of the GDPR (hereinafter "Controller data"). This agreement specifies the parties' respective rights and obligations in this regard pursuant to Art. 28 GDPR.

1.2 The term of this AVV corresponds to the term of the main contract. It ends automatically upon termination thereof, without prejudice to continuing obligations under Section 9.

2 Nature and purpose of processing, categories of data subjects and types of data

2.1 **Nature and purpose of processing:** Automated analysis of documents uploaded by the Controller using AI language models and provision of the analysis results via the platform.

2.2 **Categories of data subjects:** Employees, customers, contractual partners, or other natural persons whose data is contained in documents uploaded by the Controller.

2.3 **Categories of personal data:** Master and contact data, contract and billing data, information on employment, role, and qualifications, contents of correspondence and minutes, and any other information contained in the uploaded documents. In addition, the name and email address of persons whom the Controller invites to projects, and their comments and edits in the projects. Special categories of personal data pursuant to Art. 9(1) GDPR may not be uploaded. The Controller represents that uploaded documents do not contain such data. The other types of data follow from each uploaded document and are determined by the Controller.

2.4 The Controller may not place special categories of personal data within the meaning of Art. 9(1) GDPR on the platform. Separate consent for this is not provided.

2.5 The Processor may produce aggregated metrics for its own operations that contain no document content and no personal data, namely runtimes, error rates, and classification statistics. These metrics are not Controller data. Uploaded documents and analysis results are not evaluated for the Processor's own purposes.

3 Obligations of the Processor

3.1 The Processor processes Controller data only on documented instructions from the Controller unless required to do so by Union or Member State law; in that case the Processor informs the Controller before processing, where legally permitted.

3.2 The Processor ensures that persons authorised to process Controller data have committed themselves to confidentiality or are subject to an appropriate statutory duty of secrecy.

3.3 The Processor implements the technical and organisational measures described in **Annex 1** pursuant to Art. 32 GDPR.

3.4 The Processor supports the Controller, within its capabilities, in fulfilling data subject rights (access, rectification, erasure, restriction, data portability) and in data protection impact assessments, where required.

3.5 The Processor notifies the Controller of breaches of personal data protection without undue delay, at the latest within 48 hours of becoming aware, with the information required for the Controller to fulfil its notification obligations under Art. 33 and 34 GDPR.

3.6 Until the main contract ends and during the period under § 10(3) GTC, the Controller can download its data using the export functions of the platform. This fulfils the return. No later than 30 days after termination of the main contract, the Processor deletes all Controller data unless statutory retention obligations require otherwise. Backups are overwritten after 30 days.

4 Controller's right to issue instructions

4.1 Instructions are given via the functions provided on the platform for this purpose or in text form. The Controller bears responsibility for the lawfulness of its instructions.

4.2 If the Processor considers an instruction unlawful, it informs the Controller without undue delay and is entitled to suspend its execution pending clarification.

5 Technical and organisational measures

The technical and organisational measures taken by the Processor and its sub-processors are set out in **Annex 1**.

6 Sub-processors

6.1 The Controller hereby grants general authorisation for use of the sub-processors listed in **Annex 2**.

6.2 The Processor informs the Controller in text form of any intended addition or replacement of a sub-processor. For changes initiated by the Processor, the information is given at least 10 days before the change. For changes initiated by an existing sub-processor, the Processor informs the Controller without undue delay after becoming aware. The Controller may object to the change for an objective reason within 10 days of receiving the information. If the Processor proceeds with the change, the Controller may terminate the main contract extraordinarily with effect from the time of the change.

6.3 The Processor obliges each sub-processor under terms that ensure a level of data protection equivalent to that agreed in this AVV.

7 Controller's audit rights

7.1 Upon request, the Processor makes available to the Controller the information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR.

7.2 Evidence may be provided primarily by presenting current certifications (e.g. ISO 27001, C5 attestation of the sub-processors used) if this enables an equivalent review.

7.3 The Controller may in addition require audits, including on-site inspections. They take place during ordinary business hours after reasonable notice. The Controller bears the cost of an on-site audit unless a breach is found.

7.4 For sub-processors, the Processor provides evidence primarily through their current certifications (in particular ISO/IEC 27001) and audit reports. On-site inspections at sub-processors are governed by the conditions those sub-processors grant the Processor.

7.5 For support with data-subject requests, data protection impact assessments, audits, and the return of data, the Processor may charge reasonable remuneration unless the service was prompted by a breach by the Processor of this agreement or of applicable law. The Processor states the expected cost in advance.

8 Liability

The parties' liability is governed by statutory provisions and, supplementarily, by the liability provisions of the main contract (§ 9 GTC), unless this AVV provides otherwise.

9 Term, termination, final provisions

9.1 This AVV ends automatically upon termination of the main contract.

9.2 The obligations under Section 3.6 (deletion/return) and Section 3.5 (insofar as still relevant at the time of termination) continue beyond termination of the contract.

9.3 Amendments and supplements to this agreement require text form. This also applies to any waiver of this formal requirement.

9.4 In the event of conflicts between this AVV and the GTC, this AVV prevails on data protection matters.

9.5 In the event of discrepancies between language versions, the German version prevails.

10 Endangerment of the data by third parties

If the Controller's data held by the Processor is endangered by attachment, seizure, insolvency proceedings, or other measures by third parties, the Processor informs the Controller without undue delay. The Processor points out to everyone involved that the right to dispose of the data lies exclusively with the Controller as the controller.

Annex 1: Technical and organisational measures (TOM)

Area	Measure
Physical access control	Physical access control of the data centres for AI inference lies with IONOS Cloud GmbH and OVH SAS (OVHcloud). Physical access control of the servers for the application, database, object storage, and mail server lies with netcup GmbH in Germany.
Access control	Login with email and password (stored as hash). Optional two-factor authentication (TOTP) for users. Only administrators of the Processor have access to the systems, and only with two-factor authentication. They access the systems only to provide the service and to remedy faults.
Access authorisation control	Access via the user's own account and via project roles.
Disclosure control	Transport encryption (TLS) for all connections to the platform and to the inference providers. Document analysis is not transferred to third countries. Document content is sent only for analysis to the inference providers in Annex 2. They do not store requests permanently and are contractually obliged not to use them to train models. They record only metadata such as time, model, and token count. For IONOS Cloud, reference is made to the ISO/IEC 27001 certification published by IONOS Cloud.
Input control	Uploaded documents and jobs are assigned to the user account. Logins, failed login attempts, and account changes are logged with time and IP address.
Availability control	Backups by volume snapshots and database dumps (pg_dump). Backups are cleaned up after 30 days. Off-site storage of those backups is not warranted.
Segregation control	Separate storage per user. Projects are logically separated from one another.
Erasure	Erasure according to the periods in the GTC and the privacy policy. The Controller can delete documents itself.
Order control	Contractual binding of sub-processors (Section 6.3). The Processor updates the software in use.
Review	The Processor reviews the measures regularly, at least once a year and after material changes to the systems, and adapts them to the state of the art.

Annex 2: List of sub-processors

Sub-processor	Service	Place of processing
IONOS Cloud GmbH, Elgendorfer Str. 57, 56410 Montabaur	AI inference (AI Model Hub). If processing exclusively in Germany has been agreed on request, inference takes place only here and on the Processor's own models.	Germany

OVH SAS (OVHcloud), 2 rue Kellermann, 59100 Roubaix	AI inference (AI Endpoints), unless processing exclusively in Germany has been agreed on request	France (Gravelines)
netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe	Hosting of the application, database, and object storage; mail server for invitations and notifications	Germany

The Processor operates the application and part of the AI models itself. The measures in Annex 1 apply to them. Haufe-Lexware GmbH & Co. KG, Munzinger Straße 9, 79111 Freiburg, creates the Processor's invoices with Lexware Office. Mollie B.V. collects credit-card and SEPA direct-debit payments. Both process only the Controller's billing and payment data, for which the Processor is itself the controller, and no data from uploaded documents. They are therefore not on this list and are named in the privacy policy.