Data Processing Agreement

pursuant to Art. 28(3) GDPR

This Data Processing Agreement ('DPA') is entered into by and between the parties identified below, pursuant to Art. 28(3) of the General Data Protection Regulation (EU) 2016/679 ('GDPR').

The Contracting Parties

CONTROLLER

Company name:
[Full legal name of the Controller]

Street address:
[Street and house number]

Postal code, city:
[Postal code and city]

Country:
[Country]

Represented by:
[Name of authorised representative]

– hereinafter referred to as: Controller –

and

PROCESSOR

Company name:
4rce.com Digital Technologies GmbH

Street address:
Grafentraubach 910

Postal code, city:
84082 Laberweinting, Germany

Represented by:
Volker Geith (Managing Director)

Data protection contact:
info@4rce.com | https://aicollab.app

Commercial register: Amtsgericht Straubing, HRB 13771
VAT-ID: DE459375923

– hereinafter referred to as: Processor –

enter into the following agreement:

1. General Provisions and Subject Matter

1.1 The subject matter of this Agreement is the processing of personal data on behalf of the Controller by the Processor (Art. 28 GDPR) in connection with the use of the AI collaboration platform aicollab.app. The scope of the engagement, categories of data subjects and types of data, as well as the purpose of processing, are set out in Annex 1 to this Agreement.

1.2 The Controller is the controller within the meaning of Art. 4(7) GDPR. The Controller alone is responsible for assessing the lawfulness of processing operations under Art. 6 GDPR and for upholding the rights of data subjects.

1.3 The processing of personal data by the Processor is structured into two technically and legally distinct processing layers:

a) Data Storage (always EU): All data stored by the Controller – including chat histories, uploaded documents, user data, knowledge bases, and project content – is stored and managed exclusively on servers located in Germany (centron.de data centre, ISO 27001 certified). For data storage, without exception: processing within the meaning of Art. 44 et seq. GDPR takes place exclusively within the EU/EEA.

b) AI Model Inference (configuration-dependent): When prompts are processed by AI models, requests and outputs are routed via the AI routing service OpenRouter (openrouter.ai) to the respective AI model providers. The geographic location of this processing and the scope of data transfer to model providers depend on the following settings:

i. EU Model Routing ENABLED: Prompts and outputs are routed exclusively via Microsoft Azure AI Foundry (location: Sweden Central, Sweden/EU) as the EU model endpoint. No transfer to third countries takes place. Processing is carried out within the EU.

ii. EU Model Routing NOT enabled: Prompts and outputs may be transmitted via OpenRouter to model providers outside the EU/EEA (e.g. USA). Transfers to third countries are made on the basis of Standard Contractual Clauses (Art. 46(2)(c) GDPR) pursuant to OpenRouter's terms.

iii. ZDRP (Zero Data Retention Policy) ENABLED: OpenRouter transmits all requests to model providers with the parameter 'data_collection: deny'. Providers are thereby contractually obligated not to store prompts and outputs, nor to use them for training their models (OpenRouter Zero Data Retention). ZDRP is technically implemented via the Processor's ZDRP API key and requires an appropriate subscription tier (Pro/Teams/Enterprise).

iv. ZDRP NOT enabled (Free Tier): Model providers may use prompts and outputs for training their models in accordance with their own terms of service. The Controller bears data protection responsibility for this configuration decision.

For fully GDPR-compliant use under this DPA, the platform must be used exclusively

with ZDRP enabled and – for the processing of particularly sensitive data – additionally with EU Model Routing enabled. The Controller is responsible for the corresponding configuration in its organisation account on aicollab.app.

1.4 Remuneration is agreed separately between the parties in the applicable main agreement (service agreement / licence agreement) and is not governed by this DPA.

2. Term and Termination

This Agreement is concluded for an indefinite term and terminates automatically upon expiry of the underlying main agreement governing use of the aicollab.app platform. Either party may terminate this Agreement by giving three months' written notice. The right to terminate for cause without notice remains unaffected.

3. Instructions of the Controller

3.1 The Controller has a comprehensive right to issue instructions regarding the type, scope and modalities of data processing by the Processor. In this capacity the Controller may in particular demand the immediate deletion, rectification, restriction or return of the data that is the subject of this Agreement. The Processor is obliged to follow the Controller's instructions unless overriding contractual or statutory obligations prevent it from doing so.

3.2 The Processor shall notify the Controller without undue delay if, in its opinion, an instruction given by the Controller violates applicable law. If an instruction is issued whose lawfulness the Processor substantively doubts, the Processor is entitled to temporarily suspend execution until the Controller confirms or amends the instruction.

3.3 Instructions shall in principle be given in writing or in an electronic format (e.g. by email). Oral instructions shall, upon request by the Processor, be confirmed by the Controller in writing or in an electronic format. The Processor shall record the name of the person giving the oral instruction, the date and time in an appropriate manner.

3.4 At the request of the Processor, the Controller shall designate one or more persons authorised to give instructions. Changes shall be communicated to the Processor without undue delay.

4. Audit Rights of the Controller

4.1 The Controller is entitled to verify compliance with statutory and contractual data protection and data security requirements before the commencement of processing and regularly during the term of this Agreement, to the extent necessary, itself or through a designated third party. The Processor shall tolerate such audits and support them to the extent required. In particular, the Processor shall provide the Controller with all information necessary for the audits, completely and truthfully, grant access to stored data and data processing programmes/systems, and permit on-site inspections. Where the Controller has agreed to data processing outside the Processor's premises,

the Processor shall ensure that the Controller may also inspect those premises for audit purposes.

4.2 The Controller shall ensure that audit measures are proportionate and do not unreasonably disrupt the Processor's operations. In particular, on-site inspections should generally take place during normal business hours and with prior appointment, unless the audit purpose requires otherwise.

4.3 The results of audits and instructions shall be documented in an appropriate manner by both parties.

5. General Obligations of the Processor

5.1 Processing of the data covered by this Agreement by the Processor shall take place exclusively on the basis of the contractual arrangements in conjunction with any instructions given by the Controller. Any processing that deviates from this is only permissible on the basis of mandatory European or Member State legislation.

5.2 The Processor shall comply with all applicable laws when performing the Agreement. In particular, it shall have implemented the technical and organisational measures required under Art. 32 GDPR and shall maintain the record of processing activities required under Art. 30(2) GDPR.

5.3 Where the Processor is required by applicable law to appoint a Data Protection Officer, it confirms that it has appointed one in compliance with the law and undertakes to inform the Controller of the DPO's contact details (e.g. by email). Any changes to the person or contact details of the DPO shall be communicated to the Controller without undue delay.

5.4 Processing outside the Processor's premises or the premises of sub-processors, and/or at private residences (e.g. remote access or home office), is only permitted with the Controller's express prior consent.

5.5 The Processor shall ensure that persons authorised to process personal data have committed themselves to confidentiality or are subject to an appropriate statutory obligation of secrecy (Art. 28(3)(b) GDPR). Authorised persons shall not be granted access to the personal data provided by the Controller prior to making such a commitment.

5.6 The Processor shall regularly and independently monitor compliance with its obligations and document such monitoring in an appropriate manner.

6. Technical and Organisational Measures

6.1 The Processor has established appropriate technical and organisational measures to ensure an adequate level of protection and has set these out in Annex 2 to this Agreement. The measures described therein were selected in accordance with the requirements of Art. 32 GDPR.

6.2 The Processor shall review and adapt the technical and organisational measures as required and/or when triggered by a specific event. Required adaptations shall be documented by the Processor and made available to the Controller upon request. Material changes that could reduce the level of protection shall be agreed with the Controller in advance.

7. Assistance Obligations of the Processor

7.1 The Processor shall assist the Controller pursuant to Art. 28(3)(e) GDPR in fulfilling its obligations to uphold data subjects' rights under Chapter III, Art. 12–22 GDPR. This applies in particular to the provision of information and to the erasure, rectification or

restriction of personal data. The scope of the obligation to assist shall be determined on a case-by-case basis, taking into account the nature of the processing.

7.2 The Processor shall further assist the Controller pursuant to Art. 28(3)(f) GDPR in fulfilling its obligations under Art. 32–36 GDPR (in particular notification obligations). The scope of this obligation shall be determined on a case-by-case basis, taking into account the nature of the processing and the information available to the Processor.

8. Engagement of Sub-processors

8.1 The Processor is only authorised to engage sub-processors with the Controller's consent. All sub-processing relationships existing at the time of conclusion of this Agreement are listed in Annex 3 to this Agreement. By signing this Agreement, the Controller grants its consent to the engagement of the sub-processors listed in Annex 3. If the Processor intends to engage additional sub-processors, it shall notify the Controller in writing or electronically, so that the Controller can review their engagement.

8.2 Sub-processors shall be selected by the Processor in compliance with statutory and contractual requirements. Ancillary services used by the Processor in the ordinary course of business (e.g. telecommunications, postal and transport services, maintenance and user support) do not constitute sub-processing relationships.

8.3 All agreements between the Processor and sub-processors must meet the requirements of this Agreement and the statutory provisions governing the processing of personal data on behalf of others; this applies in particular to the implementation of appropriate technical and organisational measures under Art. 32 GDPR at the sub-processor's site.

8.4 The agreement with the sub-processor must specify the sub-processor's responsibilities so that the Controller is able to verify compliance accordingly.

8.5 Data may only be transferred to the sub-processor once the sub-processor has fulfilled its obligations under Art. 32(4) and Art. 29 GDPR towards persons under its authority.

8.6 The Processor is responsible for compliance with data protection provisions by its sub-processors. It is liable to the Controller for compliance with statutory and contractual data protection obligations by its sub-processors.

8.7 The Processor shall obtain confirmation from its sub-processors that they have appointed a Data Protection Officer where required by law.

8.8 The engagement of sub-processors in third countries is only permitted where the legal requirements of Art. 44 et seq. GDPR are satisfied and the Controller has given its consent.

9. Notification Obligations of the Processor

9.1 Breaches of this Agreement or of any other data protection provisions shall be reported to the Controller without undue delay; the same applies in the event of a corresponding substantiated suspicion. This obligation applies regardless of whether the breach was committed by the Processor itself, a person employed by it, a sub-processor, or any other person engaged to fulfil its contractual obligations.

9.2 The Processor is obliged to assist the Controller in fulfilling its statutory notification obligations under Art. 33 and 34 GDPR. The Processor may only make independent notifications to authorities or data subjects under Art. 33 and 34 GDPR after receiving a prior instruction from the Controller.

9.3 If a data subject, authority, or other third party contacts the Processor requesting information, rectification, restriction, or erasure, the Processor shall forward the request to the Controller without undue delay; in no event shall the Processor comply with the data subject's request without the Controller's consent.

9.4 The Processor shall inform the Controller without undue delay if any supervisory action or other measures by an authority are imminent that could also affect the processing, use or collection of personal data made available by the Controller.

10. Termination, Deletion and Return of Data

Upon completion of the processing that is the subject of this Agreement or upon termination of this Agreement, the Processor shall, at the Controller's election, delete or return all personal data, provided that no statutory obligation to retain the data continues to apply (e.g. statutory retention periods). The Controller is entitled to verify the Processor's measures in an appropriate manner. Deletion shall be confirmed by the Processor in writing upon request.

11. Data Secrecy and Confidentiality

11.1 The Processor is obliged, without time limit and beyond the end of this Agreement, to treat the personal data obtained in the context of this contractual relationship as confidential and to comply with relevant secrecy obligations to which the Controller is subject.

11.2 The Processor undertakes to familiarise its employees with the applicable data protection provisions and secrecy obligations and to bind them to confidentiality before they commence their activities with the Processor.

11.3 The Processor shall document compliance with the measures referred to in this clause in an appropriate manner. The documentation shall be provided to the Controller upon request.

12. Final Provisions

12.1 Amendments to this Agreement and supplementary agreements require written or electronic form that clearly identifies the amendment or supplement to the present terms.

12.2 Should the GDPR or any other statutory provisions referenced herein be amended during the term of this Agreement, references in this Agreement shall also apply to any successor provisions.

12.3 Should any individual provisions of this Agreement be or become invalid, the validity of the remaining provisions shall not be affected.

12.4 All annexes to this Agreement form an integral part of the Agreement.

12.5 This Agreement is governed by the laws of the Federal Republic of Germany. To the extent permitted by law, the courts at the registered seat of the Processor shall have jurisdiction over any disputes arising out of or in connection with this Agreement.

Signatures

By their signatures below, the parties confirm that they have read, understood and accepted this Data Processing Agreement.

Place, Date	Place, Date
_____, _____	_____, _____
Signature (Controller)	*Signature (Processor / aicollab.app)*

Annex 1 – Service Details

This Agreement covers the following services (where applicable in conjunction with the main agreement):

- Provision and operation of the AI collaboration platform under the domain aicollab.app
- Processing of user queries (prompts) and documents through AI models in the course of platform use
- Storage of user-generated content, conversation histories, and project data on EU-based servers
- Provision of collaboration and communication features for teams and organisations
- Management of user accounts, access rights, and role assignments (user management)
- Generation and storage of AI outputs (texts, summaries, analyses) based on user requests
- Provision of technical support and maintenance services as well as security updates
- Logging of usage activities for system security and quality assurance purposes
- Processing of payment and billing data via external payment service providers (where applicable)

In the course of providing the contractual services, the following categories of data are regularly processed:

- Master data of users: name, email address, job title, department, profile information
- Authentication data: username, encrypted password, API keys, session tokens
- User-generated content: AI prompts, input text, uploaded documents, chat messages, comments, project results
- AI outputs: generated texts, summaries, analyses, and other AI-generated content
- Communication data: messages and comments within the platform
- Usage and log data: login timestamps, activity logs, error messages, API requests
- Technical data: IP addresses, browser type, operating system, device ID
- Billing data: invoice address, payment references (no full payment card data – these remain with the payment service provider)

The categories of data subjects affected by the processing are:

- Employees of the Controller (staff, managers, trainees/apprentices)
- External workers, freelancers, and collaboration partners of the Controller
- Administrators and IT personnel of the Controller
- Customers or contact persons of the Controller, where their data is entered into the platform

Purpose of processing:

Provision of the AI-assisted collaboration and analysis services agreed under this Agreement in the course of use of the aicollab.app platform by the Controller and its authorised users.

⚠ **Important Notice: GDPR-Compliant Use (ZDRP + EU Model Routing)**

Data storage: All stored data (chats, uploads, user data) always remains in Germany (centron.de, ISO 27001). This applies without exception and regardless of any setting.

For fully GDPR-compliant processing under this DPA, the following applies:

1. ZDRP (Zero Data Retention Policy) – MANDATORY: Must be enabled at the organisation level. Only then does OpenRouter transmit all AI requests to model providers with 'data_collection: deny', ensuring that prompts and outputs are not used for model training. In the Free Tier (without ZDRP), model providers may use data for training pursuant to their own terms.

2. EU Model Routing – RECOMMENDED for sensitive data: Ensures that AI requests are routed exclusively through EU-based model endpoints. Without EU Routing, prompts may be transmitted via OpenRouter to providers outside the EU/EEA (e.g. USA) (basis: Standard Contractual Clauses pursuant to Art. 46 GDPR).

Without active ZDRP, use of the platform under this DPA is not permitted. The Controller is responsible for the correct configuration.

Configuration path in aicollab.app: Organisation Settings → Privacy → Enable ZDRP & Enforce EU Model Routing (both options must be set to 'Enforce for all members').

Annex 2 – Technical and Organisational Measures (TOMs) pursuant to Art. 32 GDPR

The Processor (aicollab.app) implements the following technical and organisational measures to protect the personal data covered by this Agreement. The measures have been established in accordance with Art. 32 GDPR.

I. Purpose Limitation and Data Separation

- ✓ Logical tenant separation (software-based) – strict separation of customer data
- ✓ Permission concept with role-based access control (RBAC)
- ✓ Separation of production and test systems
- ✓ Encryption of data sets to prevent unauthorised attribution

II. Confidentiality and Integrity

1. Encryption

- ✓ Transport encryption: TLS 1.3 for all data transmissions between client and server
- ✓ Encryption at rest: AES-256-bit for all stored data and database volumes
- ✓ End-to-end encrypted communication for sensitive transmissions

2. Pseudonymisation

- ✓ Pseudonymisation of log and analytics data by hashing IP addresses
- Full pseudonymisation of personal data available upon specific request

3. Physical Access Control (Data Centre)

- ✓ Automated access control system at the data centre provider (ISO 27001 certified)
- ✓ Chip card / transponder locking system
- ✓ Video surveillance of entry points
- ✓ Personnel control at reception / visitor management
- ✓ Alarm system and security personnel

4. Logical Access Control

- ✓ Assignment of user rights and creation of user profiles
- ✓ Password policies (minimum 12 characters, complexity requirements, regular changes)
- ✓ Multi-factor authentication (MFA/2FA) for all administrator access
- ✓ Hardware and software firewall in use
- ✓ VPN-secured remote access for administrative tasks
- ✓ Automatic session lock after inactivity
- ✓ Encryption of mobile storage media and laptops

5. Data Access Control

- ✓ Permission concept based on the principle of least privilege
- ✓ Management of rights by system administrators
- ✓ Regular review and update of access rights (in particular upon leaving the organisation)
- ✓ Number of administrator accounts reduced to the minimum necessary
- ✓ Logging of access to applications, particularly in the event of entry, modification and deletion
- ✓ Physical deletion of storage media before re-use (DIN 66399)

6. Input Control

- ✓ Logging of data entry, modification and deletion with timestamp
- ✓ Traceability through individual usernames (not user groups)
- ✓ Assignment of rights to enter, modify and delete data on the basis of the permission concept

7. Sub-processor Control

- ✓ Selection of sub-processors with due regard to data security
- ✓ Prior review and documentation of security measures implemented by sub-processors
- ✓ Written instructions to sub-processors (data processing agreement)
- ✓ Sub-processor employees bound to data secrecy
- ✓ Effective audit rights agreed with sub-processors

8. Transmission and Transfer Control

- ✓ TLS encryption of all communication channels (HTTPS/TLS 1.3)
- ✓ VPN tunnel for internal communication and administrative access
- ✓ No transmission of personal data via unencrypted email
- ✓ Platform data (conversation histories, user data) stored on EU-based servers
- ⚠ AI model requests (prompts/outputs): EU processing ONLY when EU Model Routing is enabled at organisation level – otherwise possible processing in third countries (USA) on basis of SCCs

9. ZDRP (Zero Data Retention Policy) – AI Model Training

- ✓ ZDRP feature available: When enabled by the Controller, AI model providers are contractually obligated not to use prompts and outputs for training their models
- ✓ ZDRP agreements in place with EU-capable model providers (where available)
- ⚠ Without ZDRP enabled by the Controller: AI model providers may use inputs/outputs for model training pursuant to their own terms – data protection responsibility rests with the Controller for this configuration decision
- ✓ ZDRP status per organisation visible and enforceable in the aicollab.app administration interface ('Enforce for all members')

III. Availability, Recoverability and Resilience

- ✓ Backup and recovery concept in place and regularly tested
- ✓ Automatic daily backups on geographically distributed systems
- ✓ System availability monitoring with automated alerting
- ✓ Incident response / business continuity plan for critical system failures
- ✓ Robust data backup and recovery concept
- ✓ Fire and smoke detection systems and fire extinguishers in server rooms (at data centre provider)
- ✓ Uninterruptible power supply (UPS) at the data centre provider
- ✓ Server rooms not located below sanitary facilities or in flood-risk areas

IV. Special Data Protection Measures

- ✓ Written data security concept in place
- ✓ Regular risk assessments conducted
- ✓ Data Protection Impact Assessment (DPIA) for high-risk processing activities
- ✓ Privacy by Design and Privacy by Default as core principles of platform development
- ✓ Privacy guardrails for AI processing implemented
- ✓ Regular employee training on data protection and information security

V. Review, Evaluation and Adaptation of Measures

The Processor shall review, evaluate and, where necessary, adapt the technical and organisational measures set out in this Annex at intervals of 12 months and on a case-by-case basis.

Annex 3 – List of Sub-processors at Time of Conclusion of Agreement

The following sub-processors are engaged at the time of conclusion of this Agreement. By signing this Agreement, the Controller grants its consent to the engagement of these sub-processors:

Note on sub-processor categories: Category A sub-processors are always active. Category B sub-processors (AI model providers) are only involved in the processing of personal data when the Controller has NOT enabled ZDRP + EU Model Routing; when EU Model Routing is active, only EU-capable endpoints are used.

Sub-processor / Address	Processing Activity	Location
CATEGORY A – Always Active (Platform Infrastructure)		
centron GmbH (centron.de) Heganger 29 D-96103 Hallstadt info@centron.de ISO 27001 certified	Server infrastructure, hosting, data storage, network operations of the aicollab.app platform in Germany. Data centre Hallstadt/Bamberg, ISO 27001 certified.	Germany (Hallstadt / Bamberg)
Supabase, Inc. (supabase.com) 65 Chulia Street #38-02/03 OCBC Centre Singapore 049513	Database service (PostgreSQL): storage of user data, organisation data, project configurations and usage data. Operated with a European database region. Basis: Standard Contractual Clauses (Art. 46(2)(c) GDPR).	EU (European region)
Cloudflare, Inc. (cloudflare.com) 101 Townsend St San Francisco, CA 94107, USA	CDN (Content Delivery Network), DDoS protection, DNS services, TLS termination and Web Application Firewall (WAF) for aicollab.app. Data is processed only temporarily as transit traffic, not stored persistently. Basis: Standard Contractual Clauses (Art. 46(2)(c) GDPR).	USA / Global (SCC per Art. 46 GDPR)
TecSpace GmbH Süsterfeldstr. 25 D-52072 Aachen info@tecspace.de HRB 18160, AG Aachen Managing Director: André Matus DPO: datenschutz@tecspace.de	Sending of transactional emails (registration, notifications, password reset, invoices). Hosted in Germany / EU.	Germany / EU
Freemius Inc.	Payment processing as	USA

(freemius.com) 4023 Kennett Pike Wilmington, DE 19807, USA Merchant of Record (MoR)	Merchant of Record: invoicing, taxes, payment management (subscriptions, licences). Freemius acts as an independent merchant; basis: Standard Contractual Clauses (Art. 46(2)(c) GDPR).	(SCC per Art. 46 GDPR)
Stripe, Inc. (stripe.com) 354 Oyster Point Blvd South San Francisco, CA 94080, USA (Payment infrastructure via Freemius)	Technical payment infrastructure for card and bank payments (engaged by Freemius as MoR). Stripe does not store complete payment data of the Controller at aicollab.app. Basis: Standard Contractual Clauses (Art. 46(2)(c) GDPR).	USA (SCC per Art. 46 GDPR)
CATEGORY B – AI Model Providers (depending on ZDRP + EU Routing configuration)		
Microsoft Corporation (Azure AI Foundry) One Microsoft Way Redmond, WA 98052, USA – ONLY when EU Routing is enabled – (Data processing: Sweden Central, EU)	EU model endpoint via Azure AI Foundry (region: Sweden Central). Processing of AI prompts/outputs exclusively within the EU. Azure data protection commitment: GDPR compliant. ZDRP: via OpenRouter 'data_collection: deny' – no use for model training.	Sweden / EU (Azure Sweden Central)
OpenRouter, Inc. (openrouter.ai) 169 Madison Avenue New York, NY 10016, USA – ONLY without EU Routing (standard mode) –	AI model routing to international providers (e.g. OpenAI, Anthropic, Google, Meta, etc.) without EU endpoints. With ZDRP: 'data_collection: deny' – no use for model training. Without ZDRP: model training by providers possible. Basis: Standard Contractual Clauses (Art. 46(2)(c) GDPR).	USA / International (SCC per Art. 46 GDPR)

Note: The Processor shall inform the Controller of planned changes regarding the addition or replacement of sub-processors, thereby giving the Controller the opportunity to raise objections to such changes.