Data Processing Agreement
pursuant to Art. 28 of the GDPR

between

Company: _____

Street, No.: _____

Postcode, City, Country: _____

(hereinafter referred to as the “Controller”)

and

alliantis GmbH
Ridlerstraße 57
80339 Munich
(hereinafter referred to as the “Processor”)

Preamble

A contractual relationship exists between the Controller and the Processor within the meaning of Article 28 of the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data, on the free movement of such data, and repealing Directive 95/46/EC, “GDPR”).

This Data Processing Agreement, including all annexes (hereinafter collectively referred to as the “Agreement”), specifies the data protection obligations of the parties arising from the underlying contract, the service agreement and/or the scope of work, including all annexes (hereinafter collectively referred to as the “Main Contract”). Where reference is made to the provisions of the Federal Data Protection Act (hereinafter “BDSG”), this refers to the Act Adapting Data Protection Law to Regulation (EU) 2016/679 and Implementing Directive (EU) 2016/680, as amended effective as of May 25, 2018.

The Processor undertakes to the Controller to fulfill the Main Contract and this Agreement in accordance with the following provisions:

§ 1 Scope of Application and Definitions

(1) The following provisions apply to all data processing services within the meaning of Article 28 of the GDPR that the Processor provides to the Controller on the basis of the Main Contract, as well as to all activities in which the Processor may process personal data on behalf of the Controller.

(2) Whenever the terms “data processing” or “processing” of data are used in this Agreement, they shall generally be understood to refer to the use of personal data. Data processing or the processing of data refers to any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, distribution or any other form of disclosure, the comparison or linking, the restriction, erasure or destruction.

(3) Reference is made to the other definitions in Art. 4 of the GDPR.

§ 2 Purpose and Duration of Data Processing

(1) The Processor processes personal data on behalf of and in accordance with the instructions of the Controller.

(2) The subject matter of this Agreement is the processing of personal data by the Processor in connection with the consulting, configuration, implementation and, where applicable, support services in the area of HR software and People & Culture solutions agreed in the Main Contract.

(3) The term of this Agreement corresponds to the term of the Main Contract.

(4) This Agreement cannot be terminated separately from the Main Contract. The right of either party to terminate for good cause remains unaffected. The Controller may in particular terminate for good cause if the Processor commits a serious breach of this Agreement or of mandatory data protection provisions and fails to remedy the breach within a reasonable period, generally not less than 14 days, after receipt of a written warning, unless such a warning is dispensable because the breach cannot be remedied.

§ 3 Nature and Purpose of Data Processing

The nature and purpose of the processing of personal data by the Processor are set forth in the Main Contract. This includes, among other things, the following activity(ies) and purpose(s):

- Consulting and implementation services and, if applicable, support services

Processing is carried out exclusively for the purpose of fulfilling the contractually agreed services and not for the Processor's own purposes.

§ 4 Categories of Data Subjects

Under this Agreement, personal data of the following categories of data subjects is processed:

- Job applicants
- Interns / working students
- Employees (permanent staff, apprentices, temporary workers, freelancers)
- Suppliers / subcontractors / contacts

§ 5 Type of Personal Data

The following types of data are affected by the processing:

- Personal master data (name, title, academic degree, date of birth)
- Contact information (email address, phone number, mailing address)
- Contract billing data and payment information (invoice details, bank account information, credit card information)
- Job application documents (resume, occupation, qualifications, certificates)
- Employee data
- Photos
- Electronic communication data (IP address, websites visited (if applicable), information about the device used, operating system and browser)
- Any other personnel data that is imported into the HR software at the Controller's request

§ 6 Rights and Obligations of the Controller

(1) The Controller is solely responsible for assessing the lawfulness of data processing and for safeguarding the rights of data subjects, and is therefore the controller within the meaning of Article 4(7) of the GDPR.

(2) The Controller is entitled to issue instructions regarding the nature, scope and procedures of data processing. Instructions shall generally be given in text form (e.g., by email); verbal instructions shall be confirmed by the Controller in text form without delay. Instructions that go beyond the services agreed in the Main Contract shall be treated as a request for a change of services.

(3) To the extent that the Controller deems it necessary, persons authorized to issue instructions may be designated. The Controller shall notify the Processor of this in writing or in text form. In the event of changes to these persons, the Processor shall be notified in writing or in text form, specifying the respective new person.

(4) The Controller shall inform the Processor without delay if errors or irregularities are detected in connection with the processing of personal data by the Processor.

(5) The Controller is entitled to verify compliance with the technical and organizational measures implemented by the Processor in accordance with § 8.

§ 7 Obligations of the Processor

(1) Data Processing

The Processor is obligated to process personal data exclusively in accordance with this Agreement and/or the underlying Main Contract, as well as in accordance with the instructions of the Controller. The Processor is prohibited from processing data in any manner that deviates from these provisions. The Processor is obligated not to process the data provided for any other purposes, in particular not for its own purposes. Copies or duplicates may only be made to the extent necessary to perform the agreed services, to ensure proper data processing (including backups) or to comply with statutory retention obligations.

(2) Rights of Data Subjects

a. The Processor shall assist the Controller, to the best of its ability, in fulfilling the rights of data subjects, particularly with regard to rectification, restriction of processing, erasure, notification and the provision of information. The Processor shall implement appropriate technical and organizational measures for this purpose. If the Processor collects personal data on behalf of the Controller and such data is the subject of a request for data portability pursuant to Art. 20 of the GDPR, the Processor shall, upon request, make the relevant data set available to the Controller in a structured, commonly used and machine-readable format in good time so that the Controller can meet the statutory time limits.

b. Upon instruction from the Controller, the Processor shall rectify, erase or restrict the processing of the personal data processed on its behalf. The same applies if this Agreement provides for the rectification, erasure or restriction of data processing.

c. If a data subject contacts the Processor directly to request the rectification, erasure or restriction of the processing of their data, the Processor is obligated to forward this request to the Controller immediately upon receipt.

(3) Monitoring Obligations

a. The Processor undertakes to ensure, through appropriate controls, that the personal data processed under this Agreement is processed exclusively in accordance with this Agreement and/or the Main Contract and/or the relevant instructions.

b. The Processor is obligated to organize its business and operational processes in such a way that the data it processes on behalf of the Controller is secured to the extent necessary and protected against unauthorized access by third parties. The Processor shall consult with the Controller in advance regarding any changes to the organization of data processing on behalf of the Controller that are significant to data security.

c. The Processor confirms that it has appointed a data protection officer in accordance with Art. 37 of the GDPR and, where applicable, § 38 of the BDSG, and that it monitors compliance with data protection and data security regulations with the involvement of the data protection officer. The Processor's data protection officer is:

Alina Bernhardt, ISiCO Datenschutz GmbH
Phone: +49 89 242 111-0
Reachable via compliance@alliantis.de

In the event of a change in the person serving as the data protection officer, the Processor shall notify the Controller in text form, specifying the new data protection officer.

(4) Duty to Provide Information

a. The Processor shall immediately notify the Controller if, in its opinion, an instruction issued by the Controller violates statutory provisions. The Processor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Controller.

b. When the Controller prepares the record of processing activities pursuant to Art. 30 of the GDPR, the Processor shall assist the Controller and provide the necessary information in an appropriate manner. The Processor shall also maintain its own record of all processing activities carried out on behalf of the Controller in accordance with the requirements of Art. 30(2) of the GDPR.

c. The Processor is obligated to immediately notify the Controller of any violation of data protection laws, the provisions set forth in the Main Contract and this Agreement and/or the instructions issued by the Controller, which occurred in the course of data processing by the Processor, persons employed by the Processor or other third parties entrusted with the processing.

d. In the event that the Processor determines, or facts give reason to believe, that personal data processed by the Processor on behalf of the Controller has been unlawfully disclosed or has otherwise unlawfully come to the knowledge of third parties, or that the protection of personal data has been otherwise compromised, the Processor shall notify the Controller without undue delay, where possible within 48 hours of becoming aware of it, in text form and – to the extent the information is available – regarding

– the time, nature and scope of the incident, including the estimated number of data records affected and the categories of data involved,
– any potential adverse consequences, and
– the measures it has taken to address the personal data breach immediately and prevent future occurrences.

Information that is not yet available at the time of the first notification shall be provided subsequently without undue delay. The Processor shall document the incident, including its effects and corrective measures, and shall assist the Controller in fulfilling its notification obligations pursuant to Art. 33 and 34 of the GDPR.

(5) Location of Data Processing

a. The Processor may process personal data on behalf of the Controller at its business premises and, by way of mobile working, at other locations of its employees (in particular home offices) within the European Union or the European Economic Area. The Processor shall ensure that the technical and organizational measures set forth in Annex 1 (in particular encrypted devices, secure network access, multi-factor authentication, screen lock and clean desk rules) are also complied with in mobile working. No separate consent of the Controller is required for this.

b. The processing and use of the data shall take place exclusively within the territory of the Federal Republic of Germany, in a member state of the European Union or in another contracting state to the Agreement on the European Economic Area. Any transfer to a third country may only take place if the specific requirements of Articles 44 et seq. of the

GDPR are met; the engagement of subprocessors is governed by § 9. This also applies to any data backups performed by the Processor.

c. Any transfer of or access to personal data from a country outside the European Union or the European Economic Area shall take place exclusively in compliance with the requirements of Articles 44 et seq. of the GDPR.

For each subprocessor concerned, Annex 2 of this Agreement documents the company's registered office, the specific processing and storage locations and the transfer mechanism used in each case.

If a valid adequacy decision by the European Commission pursuant to Article 45 of the GDPR exists for the respective recipient, this shall be specified as the basis for the transfer.

For transfers to the United States – provided that the respective recipient participates in the EU-U.S. Data Privacy Framework for the data processing in question and the transfer is covered by it – the European Commission's adequacy decision pursuant to Implementing Decision (EU) 2023/1795 may be relied upon.

If no relevant adequacy decision applies, the transfer is based on appropriate safeguards pursuant to Article 46 of the GDPR, in particular on the Standard Contractual Clauses adopted by the European Commission via Implementing Decision (EU) 2021/914.

The Processor must immediately notify the Controller in writing if the legal basis for data protection no longer applies and/or if it becomes apparent to the Processor that the legal basis will no longer apply before the end of the contract.

d. If the applicable legal basis for a transfer ceases to apply and the Processor is unable to establish an adequate alternative legal basis or an alternative processing within a reasonable period, the Controller is entitled to terminate the affected services for good cause.

e. If the processing of personal data takes place outside the EU, the Processor further guarantees that it has designated a representative based in the EU for the duration of the contract, provided this is required under the applicable data protection regulations. The representative is authorized, in addition to or in place of the Processor, to serve as a point of contact – particularly for supervisory authorities and data subjects – for all matters related to processing, in order to ensure compliance with data protection regulations.

(6) Deletion of Personal Data upon Termination of the Contract

Upon termination of the Main Contract, the Processor shall, at the Controller's choice, return or delete all personal data processed on behalf of the Controller, unless there is a statutory obligation to store the data. Data in backups shall be deleted within the regular backup cycles. Deletion shall be confirmed to the Controller upon request in text form. Documentation serving as proof of proper data processing may be retained by the Processor beyond the end of the contract in accordance with the applicable retention periods.

§ 8 Control Rights of the Controller

(1) The Controller is entitled to verify compliance with data protection regulations and this Agreement to the extent necessary. The Processor shall primarily provide such evidence by means of suitable documentation, certificates or reports (paragraph 5).

(2) Where such evidence is not sufficient in an individual case, the Controller may carry out on-site inspections itself or through an auditor bound to confidentiality who is not a competitor of the Processor. On-site inspections require timely prior notice (generally at least 14 days), shall take place during normal business hours without disrupting business operations, and are generally limited to once per calendar year unless there is a specific reason (e.g., a personal data breach). The confidentiality of data of other customers of the Processor shall be maintained.

(3) The Processor is obligated to provide information to the Controller to the extent necessary for the conduct of the audit.

(4) The Processor must comply with any supervisory measures taken by the data protection supervisory authority pursuant to Art. 58 of the GDPR and, where applicable, § 40 of the BDSG. The Processor shall inform the Controller immediately upon notification or upon becoming aware of the implementation of a supervisory measure, as well as in the event of any other inquiries or investigations by the data protection supervisory authority – in particular if these occur in the context of a prior consultation pursuant to Article 36 of the GDPR – provided that the measures or inquiries may relate to data processing activities that the Processor performs on behalf of the Controller.

(5) Upon request, the Processor shall demonstrate to the Controller compliance with the technical and organizational measures set forth in Annex 1. Such proof may be provided by submitting a current attestation or report from an independent body (such as an auditor, external data protection officer, inspector or external data protection auditor) and, where applicable, an appropriate certification (e.g., in accordance with BSI Basic Protection, ISO 27001 or an approved certification procedure pursuant to Art. 42 of the GDPR) or by demonstrating compliance with approved codes of conduct pursuant to Art. 40 of the GDPR. The Controller's rights of supervision pursuant to paragraph 1 remain unaffected.

§ 9 Subcontracting

(1) The Controller authorizes the Processor to engage additional processors in accordance with the following paragraphs of this § 9. This authorization constitutes a general written authorization within the meaning of Article 28(2) of the GDPR.

(2) The Processor currently works with the subprocessors listed in Annex 2 in fulfilling the contract, and the Controller agrees to their engagement.

(3) The Processor is authorized to engage additional processors or to replace those already engaged. The Processor shall inform the Controller in advance of any intended change regarding the engagement or replacement of an additional processor. The Controller may object to the intended change for important data protection reasons within 14 days of receipt of the information; if no objection is raised within this period, the change shall be deemed approved. In the event of an objection, the parties shall seek a mutually acceptable solution. If no such solution can be found, the Processor is entitled to terminate the affected services with reasonable notice.

(4) When engaging an additional processor, a level of protection comparable to that provided by this Agreement must always be ensured. The Processor is liable to the Controller for all acts and omissions of the additional processors it engages. The Controller has the right to verify for itself the suitability of the additional processors. Upon request, the Processor shall provide the Controller with the relevant data protection provisions of the subcontracting agreement; commercial terms may be redacted.

(5) In the subcontracting agreement with the subprocessor, the Processor must ensure that the provisions agreed upon between the Controller and the Processor, and, where applicable, any supplementary instructions from the Controller, apply in full to the subprocessor as well. This includes, in particular, the obligation of confidentiality, the guarantee of technical and organizational measures to ensure an appropriate level of security for the processing, cooperation in handling requests from data subjects and compliance with the agreed documentation obligations. In addition, the subcontracting agreement must grant the Controller rights of control and audit in accordance with this Agreement. The subcontracting agreement must specify the details set forth in §§ 2, 3, 4 and 5 of this Agreement in such a concrete manner that the responsibilities of the Processor and any additional processors are clearly delineated from one another. If multiple additional processors are engaged, this also applies to the responsibilities among these additional processors.

(6) The Processor shall regularly verify compliance with the obligations of the subprocessor. In particular, the Processor shall verify, in advance and regularly throughout the term of the agreement, that the subprocessor has implemented the promised and necessary technical and organizational measures to protect personal data. The Processor shall document the results of this verification and provide them to the Controller upon request.

§ 10 Confidentiality

(1) The Processor is obligated to maintain confidentiality when processing data on behalf of the Controller.

(2) The Processor warrants that it is familiar with the applicable data protection regulations and is proficient in their application.

(3) The Processor undertakes to use only employees or other agents in the performance of the contract who are bound to maintain confidentiality when handling the personal data provided to them and who have been adequately instructed in data protection requirements. Upon request, the Processor shall provide the Controller with evidence of compliance with these obligations.

(4) If the Controller is subject to other confidentiality rules, the Controller shall notify the Processor thereof. The Processor shall require its employees to comply with these confidentiality rules in accordance with the Controller's requirements.

§ 11 Technical and Organizational Measures

(1) The technical and organizational measures described in Annex 1 are hereby established as binding.

(2) The Processor shall comply with the principles of proper data processing pursuant to Article 32 in conjunction with Article 5(1) of the GDPR. The Processor shall ensure compliance with the contractually agreed and legally required data security measures. The Processor shall take all necessary measures to safeguard the data and ensure the security of the processing – in particular, taking into account the state of the art – as well as to mitigate any potential adverse consequences for data subjects. The measures to be taken include, in particular, measures to ensure appropriate pseudonymization and encryption, measures to protect the confidentiality, integrity, availability and resilience of the systems, and measures to ensure the continuity of processing following incidents. In order to ensure an appropriate level of security for the processing at all times, the Processor will regularly evaluate the implemented measures and make adjustments as necessary. The Processor may adapt the measures to technical progress,

provided that the level of protection is not reduced. Significant changes shall be documented and communicated to the Controller upon request.

§ 12 Compensation

(1) The Processor's remuneration is set forth in the underlying Main Contract.

(2) Support services pursuant to §§ 6(5), 7(2), 7(4) and 8 that go beyond the scope of the Main Contract and are not caused by a breach of this Agreement by the Processor shall be remunerated separately on the basis of the rates agreed in the Main Contract or, in the absence thereof, the Processor's prevailing rates.

§ 13 Liability

(1) The liability of the parties towards data subjects is governed by Art. 82 of the GDPR.

(2) In the internal relationship between the parties, each party shall bear damages to the extent that it is responsible for the circumstance giving rise to the damage (Art. 82(5) of the GDPR).

(3) In all other respects, the liability provisions of the Main Contract, including the limitations of liability agreed therein, shall also apply to this Agreement.

§ 14 Miscellaneous

(1) In the event of any conflict between the provisions of this Agreement and the provisions of the Main Contract regarding data protection obligations, the provisions of this Agreement shall prevail.

(2) Amendments and additions to this Agreement must be made in writing and must expressly state that they amend and/or supplement the provisions herein. This also applies to any waiver of this formal requirement.

(3) This Agreement is governed by German law.

(4) If access to the data that the Controller has transferred to the Processor for data processing is jeopardized by actions of third parties (e.g., actions by an insolvency administrator, seizure by tax authorities, etc.), the Processor must notify the Controller of this immediately.

(5) The right of retention pursuant to § 273 of the German Civil Code (BGB) is excluded with respect to the processed data and the associated data carriers.

For the Controller	**For alliantis GmbH**
Place, date: _____	Place, date: Munich, _____
_____	_____
Signature	Signature
Name, position: _____	Name, position: _____

List of Annexes

Annex 1	Technical and organizational measures taken by the Processor to ensure the security of data processing
Annex 2	Subcontracting relationships pursuant to § 9 of this Agreement

Annex 1 – Technical and Organizational Measures

See separate document “Technical and Organizational Measures (TOM) of alliantis GmbH”, as amended from time to time.

Annex 2 – Subcontracting Relationships pursuant to § 9

The Processor currently collaborates with the following additional processors in fulfilling the contract, and the Controller agrees to their engagement.

If data processing takes place outside the European Economic Area or if access occurs from outside the European Economic Area, the overview also lists the measures and safeguards that ensure an adequate level of data protection in accordance with Art. 44 et seq. of the GDPR (e.g., EU Standard Contractual Clauses, BCRs or an adequacy decision by the European Commission).

The current list of subprocessors is available at: https://alliantis.de/en/alliantis-legal-data-security-information