Agreement on contract data processing

Regarding to art. 28 - GDPR

to the contracts under the

Customer number: 342471

between

Artellico
Arsenal 3/71
1030 Wien

- hereinafter referred to as "Client" - as "controller" pursuant to Art 4 (8) GDPR

and

netcup GmbH
Emmy-Noether-Str. 10
76131 Karlsruhe

- hereinafter referred to as "Contractor" - as "processor" pursuant to Art 4 (8) GDPR

- together referred to as "Contracting Parties" or "Parties" -

Preamble

This agreement serves to supplement and specify the contractual partners' obligations regarding data protection for all existing and future legally effective contracts, master service agreements, service level agreements, service descriptions, etc. (hereinafter referred to collectively as "contract" or "contracts") between the client and the contractor It applies to all activities related to the contracts between client and contractor and in which contractors employees or persons commissioned by the contractor process personal data (hereinafter referred to as "Data") on behalf of the client as the data controller or data processor. In addition, all provisions and terms of the EU General Data Protection Regulation [Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC] (hereinafter referred to as "GDPR") apply to this document, as do the national data protection laws applicable to the contracts. For the sake of clarity and readability of this document, all person-related notations apply to members of all genders. It should be noted that the contractor, as an affiliated company of the Anexia group of companies with ANEXIA Internetdienstleistungs GmbH as the lead company (hereinafter referred to as "Anexia"), is subject to all group-wide regulations ("Anexia Corporate Binding Rules") and that the data processing that the contractor carries out for the client as the responsible party (data controller or data processor) is carried out primarily by people working for Anexia and, if necessary, by using Anexia's infrastructure and systems. The active certifications of the Anexia companies netcup GmbH, ANEXIA Internetdienstleistungs GmbH and DATASIX Rechenzentrumsbetriebs GmbH in the areas of ISO 9001 (quality management), ISO 27001 (information security) and ISO 27701 (data protection) and others are currently published on the respective company websites.

1. Subject Matter, Location and Duration of Contract Data Processing

1. The subject matter and duration of the contract, the type and purpose, the place of processing and the categories of data processed as well as the categories of data subjects are specified separately by the client in ANNEX 3.
2. The place of processing under consideration of Chapter V GDPR is decided exclusively by the AG as controller or processor.
3. The controller instructs the contractor contractually, by means of instructions or by means of ANNEX 3 to conduct the processing either exclusively within the EU or the EEA or to conduct it, partially or entirely, taking into account the applicable legal bases, in third countries to be designated by the client or at certain specific locations to be designated by the client. The term of the contract data processing depends on the term of the contracts between the client and the contractor.

2. Scope and responsibility

1. The contractor ("processor" according to Art. 4 No. 8 GDPR) processes data on behalf of the client. This includes those activities that are specified in the contracts. Within the framework of these contracts, the client ("controller" according to Art. 4 No. 7 GDPR or "processor" according to Art. 4 No. 8 GDPR) is solely responsible for compliance with the statutory provisions on data protection, in particular for the legality of the processing itself and the transfer of data to the contractor as the processor or sub-processor.

2. The client's instructions are set out in the contracts and can be changed, supplemented, or replaced by the client in writing or in a documented electronic format to the contractor by individual instructions. Any verbal instructions must be confirmed immediately in writing in text form. All instructions given must be documented by the client and kept for the duration of their validity and then for a further three full calendar years. Instructions that go beyond the contractual agreements and are not necessary to prevent or remedy legal violations in the contractor's area of responsibility may be subject to a fee.

3. Obligations of the Contractor as a Processor

1. The contractor may only collect, use, or otherwise process data within the framework of the contracts and in accordance with the instructions of the client; this applies in particular with regards to the transfer of personal data to a third country or to an international organization. If the contractor is required to conduct further processing by the law of the European Union or the member states to which it is subject, it will inform the client of these legal requirements before processing if the applicable law does not prohibit such notifications.

2. The contractor will inform the client immediately if it believes that an instruction from the client violates the GDPR or other data protection regulations of the European Union or member states. The contractor is entitled to suspend the implementation of the relevant instruction until it is confirmed or changed by the client. The contractor can demand appropriate security before carrying out instructions which, according to the contractor's objectively comprehensible (not necessarily correct) assessment, are unlawful and which threaten to cause damage to the contractor if they are implemented.

3. The contractor will design the internal organization within his area of responsibility in such a way that it meets the special requirements of applicable data protection regulations. He undertakes to implement all suitable technical and organizational measures to adequately protect the client's data in accordance with Art. 32 GDPR, in particular the measures listed in ANNEX 1. The contractor reserves the right to change the measures taken without separate notice, whereby the contractually agreed level of protection may not be undercut.

4. The persons of the contractor who are involved in processing the client's data are prohibited from processing the data without authorization. The contractor will oblige the aforementioned persons accordingly (obligation to maintain confidentiality, Art. 28 para. 3 lit. b GDPR). These obligations must be formulated in such a way that they continue to exist even after the termination of the collaboration with or work for the contractor and after the termination of this contract.

5. The contractor supports the client to the best of its ability in fulfilling the rights of data subjects under Chapter III of the GDPR. In addition, the contractor supports the client in complying with the obligations set out in Articles 32 to 36 of the GDPR, considering the type of processing and the information available.

6. The contractor will inform the client immediately if he becomes aware of any breaches of the client's data protection. In such cases, the contractor will take the necessary measures to secure the data (in accordance with the client's instructions) to reduce possible adverse consequences for the persons affected and will immediately consult with the client on this matter.

7. If deletion in accordance with data protection regulations or a corresponding restriction of data processing is not possible, the contractor shall undertake the destruction of any affected data media and other materials in accordance with data protection regulations based on an individual instruction from the client or shall return these data media to the client, unless otherwise agreed in the contract.

8. In special cases to be determined by the client, the data will be stored or handed over to third parties to be determined by the client, whereby remuneration and protective measures for this must be agreed separately, unless already regulated in the contracts.

9. After completion of the processing services, the contractor will either delete or return all personal data at the client's discretion and delete the existing copies, unless there is an obligation to store the personal data under European Union law or the law of the Member States or the personal data is still contained in any backups of the contractor. The personal data in any backups will be deleted after a maximum of 14 days.

10. In the event of a claim being made against the client by a data subject with regard to any claims pursuant to Art. 82 GDPR, the contractor undertakes to provide the Client with the best possible support in defending against the claim within the scope of its possibilities.

4. Obligations of the Client as Controller or Processor

1. The client as the controller or processor ensures that the processing is carried out in accordance with the principles set out in Chapter II of the GDPR and that the technical and organizational measures taken by the contractor as the processor (ANNEX 1) and any additional measures specified in the contracts provide an appropriate level of protection, taking into account the nature, scope, circumstances and purposes of the processing as well as the different likelihood and severity of the risks to the rights and freedoms of natural persons.

2. The client must inform the contractor immediately and fully if it discovers errors or irregularities regarding data protection regulations in the contract data processing results.

3. In the event of a claim against the contractor by a data subject with regard to any claims under Art. 82 GDPR, point 3.10. shall apply mutatis mutandis.

5. Data Protection Officer and Contacts

1. The contact details of the contractor's data protection officer are published on the contractor's homepage.

2. The client shall provide the contractor with one or more contact persons for all data protection issues arising within the scope of the contracts, including the present agreement:

First name	Last name	E-mail	Phone
Alexander	Pokorny	alexander.pokorny@artellico.com	+436769511853

6. Requests of Data Subjects

1. If a data subject approaches the contractor with requests under Chapter III of the GDPR (e.g., rectification, erasure, or information), the contractor will refer the data subject to the client, provided that an assignment to the client is possible based on the information provided by the data subject.

2. The contractor shall not be liable if the client does not respond to the request of the person concerned, does not respond correctly, or does not respond within the deadline.

7. Verification Options and Inspection Rights

1. Upon request, the contractor shall provide the client with all information required to demonstrate compliance with the contractor's obligations set out in Art. 28 GDPR within a reasonable period of time. To this end, the contractor may in particular submit certifications of the contractor and, if applicable, other Anexia companies and subcontractors outside the Anexia group of companies in the areas of ISO 9001 (quality management) and/or ISO 27001 (information security) and/or ISO 27701 (data protection). The contractor reserves the right to only submit certain documents after prior signing of a corresponding non-disclosure agreement (NDA), as far as these relate to confidential information of the contractor.

2. The contractor will facilitate and contribute to checks - including inspections - conducted by the client or another auditor commissioned by the client, provided that the latter is not in direct competition with the contractor. The client will only conduct checks to the extent necessary and these must not lead to an excessive disruption of the contractor's business operations. As a rule, checks can only be conducted after notification and with an appropriate lead time, unless an inspection without prior notification appears necessary because otherwise the purpose of the inspection would be jeopardized.

3. Unless the inspection was necessary due to a breach of law or contract by the contractor, the client shall bear the costs of the inspection, including the expenses incurred by the contractor in connection with the inspection.

8. Other Processors

1. The client hereby gives its consent for the contractually agreed services or the partial services described in ANNEX 2 to be carried out with the involvement of the additional processors named therein ("subcontractors").

2. Any provisions regarding subcontractors in offers or contracts between the client and the contractor shall be deemed to constitute consent by the client to the involvement of such subcontractors.

3. The contractor is authorized to establish further subcontracting relationships with subcontractors ("subcontracting relationship") within the scope of its contractual obligations. Before establishing further subcontracting relationships, the contractor informs the client in writing. The client can object to the change for objective reasons within 14 calendar days. A subcontracting relationship with another processor exists if the contractor commissions other companies to provide all or part of the service agreed in the contracts between the client and the contractor, and the core activity consists in processing personal data of the client as the controller or processor. The mere provision of subordinate ancillary services where the core activity does not lie in the processing of personal data (e.g., pure infrastructure provision, telecommunications, postal or cleaning services, security guards) is not a subcontracting relationship.

4. If the contractor uses the services of a subcontractor to conduct certain processing activities on behalf of the client, the contractor is obliged to fully transfer all legal and contractual data protection obligations to which it is subject towards the client to these additional processors, whereby in particular sufficient guarantees must be provided that the appropriate technical and organizational measures are implemented in such a way that the processing is carried out in accordance with the requirements of the GDPR.

9. Information Obligations, Written Form, Severability Clause and Choice of Law

1. If the client's data is at risk through seizure or confiscation, through insolvency or composition proceedings or through other events or measures by third parties, the contractor must inform the client immediately. The contractor will immediately inform all those acting in this context that sovereignty and ownership of the data lies exclusively with the client as the controller or the clients client if the client acts as a processor within the meaning of the GDPR.

2. Changes and additions to this agreement and all its components must be made in writing or in a documented electronic format. This also applies to the waiver of this formal requirement.

3. In the event of any contradictions or ambiguities regarding data protection law, the provisions of this agreement on data protection take precedence over the provisions of the contracts. Should individual provisions of this agreement be or become invalid or unenforceable in whole or in part, this shall not affect the validity of the remaining provisions.

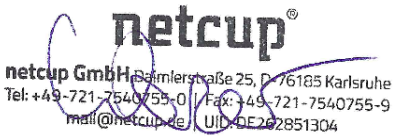
4. German law applies.

10. Liability and Compensation

The client undertakes to indemnify and hold the contractor harmless from any claims by third parties in connection with a breach of data protection regulations caused by the client. Otherwise, Art. 82 GDPR applies.

11. Confidentiality and Non-disclosure

Both parties undertake to maintain basic confidentiality and secrecy with regard to the contents of this agreement. This does not include statutory disclosure obligations to authorities, in court or criminal proceedings, or contractual obligations to persons and auditors of both the client and the contractor who undertake to maintain confidentiality towards the client or the contractor or who are subject to a professional or confidentiality obligation, the violation of which is punishable under the Criminal Code, and ultimately also other processors and affiliated companies for whom the provisions in question represent an integral part of the performance of their activities.

Client	Contractor
	Karlsruhe, 12.01.2026
Place, Date	Place, Date
	
	Oliver Werner
Signature	Signature

Attachments

☑ ANNEX 1 - Technical and organisational measures (TOM)

☑ ANNEX 2 - Further other processors

☑ ANNEX 3 - Processing specifications (optional)

DPA ANNEX 1

Technical and organizational measures (TOM)

The present document supplements the Data Processing Agreement (DPA) between Client and Contractor pursuant to Art 28 GDPR (EU General Data Protection Regulation). The technical and organizational measures are implemented by Anexia in accordance with Art 32 DSGVO. They are continuously improved by Anexia according to feasibility and state of the art - not least also in terms of the active ISO 27001 certification - and brought to a higher level of security and protection.

1. Confidentiality

1. **Physical Access Control**

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

1. **Office location Karlsruhe**

Technical Measures	Organizational Measures
☑ Alarm system	☑ Key regulation / list
☑ Manual locking system	☑ Visitor book / Visitor log
☑ Doors with knobs on the outside	☑ Employee / Visitor badges
	☑ Visitors accompanied by staff
	☑ Carefulness in selecting cleaning services

2. **Data center location Nuremberg**

Technical Measures	Organizational Measures
☑ Alarm system	☑ Key regulation / list
☑ Chip cards / Transponder systems	☑ Employee / Visitor badges
☑ Doors with knobs on the outside	☑ Visitors accompanied by staff
☑ doorbell system with camera	☑ Carefulness in selecting cleaning services
☑ Video surveillance	

3. **Data center location Vienna**

Technical Measures	Organizational Measures
☑ Alarm system	☑ Key regulation / list
☑ Biometric access control	☑ Visitor log
☑ Chip cards / Transponder systems	☑ Employee / Visitor badges
☑ Doors with knobs on the outside	☑ Visitors accompanied by staff
☑ Video surveillance of the entrances	☑ Carefulness in selecting cleaning services

2. **Logical Access Control**

Measures designed to prevent data processing systems from being used by unauthorized persons.

Technical Measures	Organizational Measures
☑ Login with username + strong password	☑ User permission management
☑ Anti-virus software server	☑ Central creation of user profiles
☑ Anti-virus software clients	☑ Password-protected user accounts
☑ Firewall	☑ Application of state-of-the-art security measures for teleworking
☑ IDS in use (Intrusion Detection Systems)	☑ Restricted use of administrative user accounts
☑ IPS in use (Intrusion Prevention Systems)	
☑ Use of VPN for remote access	
☑ Encryption smartphones	
☑ Automatic desktop lock	
☑ Encryption of hard drives on notebooks / tablets / smartphones	
☑ Two-factor authentication in data center operations and critical systems	

3. **Authorization Control**

Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use and after storage.

Technical Measures	Organizational Measures
☑ Document shredder at least recommended security level P-4 (DIN 66399)	☑ Use of authorization concepts
☑ Physical deletion of data storage devices security level H-4 (DIN66399)	☑ Minimum number of administrators
☑ Logging of access to applications, specifically when entering, changing, and deleting data	☑ Administration of user rights by administrators
☑ Access to systems via SSH	☑ Application of cryptographic methods according to the current state of the art
☑ TLS encryption	

4. **Separation Control**

Measures to ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logically and physically separating the data.

Technical Measures	Organizational Measures
☑ Separation of production and test environments	☑ Definition of database rights
☑ Physical separation (systems / databases / data carriers)	☑ Defined requirements for development environments
☑ Multi-tenancy of relevant applications	
☑ VLAN segmentation of networks	
☑ Customer systems logically separated	
☑ Staging of development, test, and production environments	

2. Integrity

1. **Transfer Control**

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

Technical Measures	Organizational Measures
☑ Use of VPN	☑ Implementation of the need-to-know principle
☑ Logging of accesses and retrievals	
☑ Provisioning via encrypted connections such as sftp, https – Secure Cloudstores	
☑ Technical logging of input, modification, and deletion of data	

3. Availability and Resilience

1. **Availability Control**

Measures to ensure that personal data is protected against destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, RAID systems, disk mirroring, etc.).

Technical Measures	Organizational Measures
☑ Fire and smoke detection systems	☑ Existing emergency preparedness planning
☑ Fire extinguisher server room	☑ Regular tests of the RZ diesel generators
☑ Server room monitoring temperature and humidity	
☑ Air-conditioned server room	
☑ UPS system and emergency diesel generators RZ	
☑ Protective power strips server room	
☑ RAID system / hard disk mirroring	
☑ Video surveillance server room	
☑ Use of protection programs against malware	

2. **Recoverability Control**

Measures to enable the availability of and access to personal data to be restored quickly in the event of a physical or technical incident.

Technical Measures	Organizational Measures
☑ Backup monitoring and reporting	☑ Recovery concept
☑ Restorability from automation tools	☑ Control of the backup process
☑ Backup concept according to criticality and customer specifications	☑ Regular testing of data recovery and logging of results
	☑ Storage of backup media in a safe place outside the server room

4. Procedures for regular Review, Assessment and Evaluation

1. **Data Protection Management**

Technical Measures	Organizational Measures
☑ Central documentation of all data protection regulations with technical access for employees	☑ Data protection management system implemented
☑ Annual review of the adequacy of the TOM	☑ Information security management implemented

2. **Incident Response Management**

Support in security breach response and data breach process.

Technical Measures	Organizational Measures
☑ Use of firewall and regular updates	☑ Documented procedure for dealing with security and data protection incidents
☑ Use of spam filters and regular updates	☑ Documentation of security incidents and data breaches via ticket system
☑ Use of virus scanners and regular updates	
☑ Intrusion Detection System (IDS) for customer systems on request	
☑ Intrusion Prevention System (IPS) for customer systems on request	

3. **Privacy-friendly default settings**

"Privacy by design" / "Privacy by default" according to Art 25 Paragraphs 1 and 2 GDPR.

Technical Measures	Organizational Measures
☑ Consideration of the principles of “data protection by design” and “data protection by default” in software development	

4. **Order control (outsourcing, subcontractors, and contract data processing)**

Measures to ensure that personal data processed on behalf of the controller can only be processed in accordance with the instructions of the controller.

Technical Measures	Organizational Measures
☑ Monitoring of remote access by external parties, e.g., in the context of remote support	☑ Supplier evaluations are carried out on a risk-based basis
☑ Monitoring of subcontractors according to the principles and technologies set out in previous chapters 1, 2	☑ Prior review of the safety measures taken by the contractor and their documentation
	☑ Selection of the contractor based on defined criteria
	☑ Conclusion of the necessary agreement for contract data processing
	☑ Framework agreement for contract data processing within the group of companies
	☑ Regular review of the contractor and his level of protection

5. Technical and organizational measures of infrastructure-providing subcontractors

The contractor uses colocation data center service providers as subcontractors in the operational and business sense. These are not "additional processors" as defined by the GDPR, as their core activity never involves the processing of personal data, but rather a so-called subordinate ancillary service in the form of infrastructure provision.
Due to the information security relevance for the Contractor and the Client - especially with regard to availability - the Contractor only uses carefully selected companies for these secondary activities and regularly checks them.

6. Certifications

Both the quality management system according to ISO 9001 and the information security management system according to ISO 27001 of netcup GmbH and significant parts of the Anexia group of companies including DATASIX data center operations are certified by the independent TÜV NORD CERT GmbH. In addition, the data protection management system according to ISO 27701 of netcup GmbH and significant parts of the Anexia group of companies including DATASIX data center operations are certified by the independent CIS - Certification & Information Security Services GmbH.

DPA ANNEX 2

☑ **ANX Holding GmbH**, Feldkirchner Straße 140, 9020 Klagenfurt, Austria; **Contract content**: Provision of support services in various areas (e.g., regulatory inquiries, billing, etc.)

☑ **ANEXIA Internetdienstleistungs GmbH**, Feldkirchner Straße 140, 9020 Klagenfurt, Austria; **Contract content**: Provision of infrastructure services in the data center environment and provision of personnel

☑ **ANEXIA Deutschland GmbH**, Emmy-Noether-Straße 10, 76131 Karlsruhe, Germany; **Contract content**: Provision of infrastructure services in the data center environment and provision of personnel

DPA ANNEX 3 (optional)

Processing specifications

1. Subject (Nature & Purpose) of the Processing

☑ The processing by the Contractor for the Client as the controller has the **following specific subject matter**:

Subject matter of the processing: The subject matter is the provision of technical infrastructure services (Infrastructure as a Service / IaaS) by the Processor, comprising virtualized server capacities, physical storage, and network connectivity.

Purpose of the processing: The purpose is the technical hosting and operation of a Software-as-a-Service (SaaS) platform controlled by the Client ("Artellico"). This includes the storage and processing of data within databases (specifically relational and vector-based systems), the execution of application environments (e.g., containerized applications), and the maintenance of system availability and backups to serve end-users in the field of academic consulting and knowledge management.

2. Duration of the Processing

☑ The duration of the order and the associated processing by the Contractor for the Client as the controller or processor specifically results from the existing contracts between the parties.

3. Location of the Processing

☑ The location of the contract data processing by the contractor for the client as the controller or processor arises specifically from the existing contracts between the parties.

4. Categories of Data Subjects

☑ Data of the **following categories of data subjects** (natural persons) are processed:

- ☑ Customers
- ☑ Employees of the Client
- ☑ Interested parties
- ☐ External employees
- ☐ Suppliers
- ☐ Data processors, other processors
- ☑ Visitors to the website
- ☑ Newsletter subscribers

☐ Additional data (One per line)

---

5. Categories of Personal Data

☑ Data of the **following categories of personal data** are processed:

- ☑ Name data
- ☑ Contact and address data
- ☐ Date of birth
- ☑ Customer contract data
- ☑ Bank and payment data
- ☑ Login and authentication
- ☑ Location and geographic information data
- ☑ Preference and behavior data
- ☑ Education data
- ☐ Motion profile data
- ☑ Traffic data
- ☑ Photo, video, or audio data
- ☐ Data relevant to criminal law

☐ Additional data (One per line)

---

and/or

☑ **No special categories of personal data** ("sensitive data") according to Art 9 GDPR are processed.

or

☐ **The following special categories of personal data** according to Art 9 GDPR are processed:

- ☐ Racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Genetic data
- ☐ Data concerning health
- ☐ Biometric data
- ☐ Data concerning sex life or sexual orientation