anexia

—

COMMISSIONED DATA PROCESSING AGREEMENT

—

COMMISSIONED DATA PROCESSING AGREEMENT

between

ANEXIA Deutschland GmbH
Konrad-Zuse-Platz 8
81829 Munich
Germany
– hereinafter referred to as “Anexia” –

and

Company name
Street
Town/city, zip code
Country
– hereinafter referred to as the “Client” –

– together referred to as the Contracting Partners or Parties –

PREAMBLE

This document consolidates the obligations of the Contracting Parties regarding data protection, building on all existing and future contracts between the Client and Anexia. It applies to all activities related to existing and future contracts between the Client and Anexia and in which employees of Anexia or persons commissioned by Anexia process the personal data (“Data”) of the Client.

§1 Subject, duration and specification of the commissioned processing

The subject and duration of the commission and the type and purpose of the processing are based on the contracts. In particular, the following data is involved in data processing:

Type of data	Type and purpose of data processing	Categories of data subjects

The term of this document is determined by the term of the contracts, insofar as no additional obligations result from the provisions of this document.

§2 Area of application and responsibility

1. Anexia shall process personal data on behalf of the Client. This comprises activities that are specified in the contracts and in the service description. Within the framework of those contracts, the Client is solely responsible for compliance with the statutory provisions of data protection legislation, in particular for the legal admissibility of data transfer to Anexia and for the legal admissibility of the data processing ("Controller" within the meaning of Art. 4 (7) GDPR).

2. The instructions are initially defined by the contracts and may subsequently be modified, extended or replaced by individual instructions in written form or in an electronic format (text form) from the Client to the office designated by Anexia. Instructions that are not included in the contract shall be treated as an application to modify the service. Verbal instructions shall be confirmed immediately in writing or in text form.

§3 Obligations of Anexia

1. Anexia may process data of data subjects only within the framework of the commission and instructions of the Client, except in exceptional cases within the meaning of Article 28 (3a) GDPR. Anexia shall inform the Client immediately if it is of the opinion that an instruction breaches applicable legislation. Anexia may suspend implementation of the instruction until it is confirmed or modified by the Client.

2. Anexia shall arrange the internal organization in its area of responsibility in such a way that it meets the particular requirements of data protection. Anexia shall implement technical and organizational measures to provide appropriate protection of the Client's data that satisfy the requirements of the General Data Protection Regulation (Art. 32 GDPR). Anexia shall implement technical and organizational measures that permanently ensure the confidentiality, integrity, availability and capacity of the systems and services in relation to processing. The Client is aware of these technical and organizational measures (see §8) and it is responsible for ensuring that they offer an appropriate level of protection for the risks relating to the data to be processed.

   In relation to compliance with the agreed protective measures and their verified effectiveness, reference is made to the active ISO 9001 and ISO 27001 certification from TÜV Nord, the certificate for which shall suffice the Client as evidence of appropriate guarantees. The certificate is available on request or on the Anexia website.

   Anexia reserves the right to change the safety measures taken, although it must be ensured that the contractually agreed level of protection is maintained.

3. If agreed, Anexia shall support the Client as far as possible in fulfilling the requests and claims of data subjects pursuant to Section III of the GDPR and in complying with the obligations specified in Art. 33 to 36 GDPR. Anexia is entitled to invoice the Client for costs incurred in this connection, subject to prior notice.

4. Anexia guarantees that the employees involved in processing the Client's data and other persons who work for Anexia are forbidden from processing the data beyond the instructions. Anexia further guarantees that the persons authorized to process the personal data have undertaken to maintain confidentiality or are under an appropriate statutory confidentiality obligation. The confidentiality / secrecy obligation shall continue after the contract has come to an end.

5. Anexia shall notify the Client immediately if it becomes aware of breaches in the protection of the Client's personal data. Anexia shall implement the measures required to safeguard the data (in accordance with the Client's commission) and to reduce potentially negative consequences for the data subject and shall consult the Client about this immediately.

6. The Client's questions about data protection shall be submitted to the relevant office at Anexia by email to privacy-protection@anexia-it.com. Questions about the GDPR may be directed to dsgvo@anexia-it.com.

7. Anexia guarantees that it shall meet its obligations under Art. 32 (1) letter d) GDPR in employing a procedure for regular checking of the effectiveness of the technical and organizational measures that ensure the security of processing. This is guaranteed by successful certification in accordance with ISO 9001 and ISO 27001 by TÜV Nord.

8. Anexia shall correct or erase the data covered by the contract if the Client instructs it to do so and if this falls within the framework of the instructions. If erasure in accordance with data protection or a corresponding restriction of data processing is not possible, Anexia shall destroy the data carriers and other materials relating to an individual commission by the Client in accordance with data protection or shall return those data carriers to the Client, if this has not already been agreed in the contract. Anexia is entitled to invoice the Client for costs incurred in this connection, subject to prior notice.

In specific cases to be defined by the Client, data shall be stored or transferred; remuneration and protective measures in this connection shall be agreed separately, if not already agreed in the contract.

9. Data, data carriers and all other materials shall either be released or erased at the end of the contract on demand by the Client. In the case of test and reject materials, an individual commission is not required. If additional costs are incurred as a result of different specifications for the release or erasure of data, they shall be met by the Client.

10. In the event of a claim by a data subject against the Client regarding any rights pursuant to Art. 82 GDPR, Anexia undertakes to support the Client to the best of its ability in its defense against the claim.

§4 Obligations of the Client

1. The Client shall notify Anexia immediately and in full if it identifies faults or irregularities regarding data protection provision in the results of the commission.

2. In the event of a claim by a data subject against the Client regarding any rights pursuant to Art. 82 GDPR, Section 3 (10) shall apply accordingly.

3. The Client shall identify one or more contacts to Anexia for any data protection questions in connection with the Agreement.

First name	Surname	Email	Telephone

§5 Inquiries from data subjects

If a data subject contacts Anexia with demands for correction, deletion or information, Anexia shall refer the data subject to the Client, insofar as it is possible to associate the data subject with the Client from the information provided. Anexia shall immediately forward the data subject's application to the Client. Anexia shall support the Client to the best of its ability on instruction, to the extent agreed. Anexia shall not be liable if the request of the data subject is not answered, is not answered correctly or is not answered promptly by the Client.

§6 Verification options

1. Anexia shall verify compliance with the obligations set out in this Agreement to the Client by appropriate means.
   a) Completion of an annual self-audit by Anexia within the framework of ISO 9001 and ISO 27001 certification
   b) Certificate of information security: ISO 27001
   c) Certificate for organizational measures: ISO 9001
2. If, in individual cases, audits by the Client or by an auditor appointed by the Client are necessary, they shall be carried out during normal business hours, without disruption to operations and with prior notification, including an appropriate lead time of at least two weeks. Anexia may make this dependent on prior notification with an appropriate lead time and on signing of a confidentiality agreement regarding the data of other customers of Anexia and the technical and organizational measures that are in place. If the auditor appointed by the Client is in a competitive relationship with Anexia, Anexia has the right to object to the appointment.

   The Client shall agree to the appointment by Anexia of an independent external auditor who shall provide Anexia with a copy of the audit report.

   Anexia may demand remuneration for its support in completion of an audit. As a matter of principle, the work involved in an audit for Anexia is restricted to one day per calendar year.
3. Should a data protection supervisory authority or another supervisory authority governing the Client carry out an audit, paragraph 2 applies accordingly. It is not necessary to sign a confidentiality obligation if this supervisory authority is subject to professional or statutory confidentiality under which a breach is punishable under the Criminal Code.

§7 Subcontractors

1. The use of subcontractors as additional processors is permitted only if the Client has consented in advance. The provision on subcontractors in the quotation or Master Services Agreement between the Client and Anexia shall take precedence over the provision in this paragraph.
2. A subcontractor relationship requiring consent shall exist if Anexia appoints other contractors to carry out the whole service or part of the service agreed in the contracts between the Client and Anexia, insofar as the latter acts as the processor. Anexia shall conclude agreements with these third parties to the extent required to ensure that appropriate data protection and information security measures are in place.
3. If Alexia awards contracts to subcontractors, Anexia is obliged to transfer its legal data protection obligations under this Agreement to the subcontractor.

§8 Technical and organizational measures

The technical and organizational measures shall be implemented as appropriate by Anexia. Agreements concluded between the Client and Anexia shall take precedence over the agreements in this paragraph, provided that the technical and organizational measures are maintained.

1. Physical access control

Measures to prevent entry by unauthorized persons to data processing systems with which personal data is processed and used:

Anexia operates a multi-level entry system for the data processing systems. All employees are given adapted access cards that are only valid for their respective area. Access to the cabinet systems and access doors is only possible with individual keys or telephone numbers with sender recognition. The entire premises in which the data is processed (computer center) are protected extensively by security cameras.

2. Access control

Measures to prevent data processing systems being used by unauthorized persons:

The following security measures are carried out internally to meet the security standards:

- *Access to the server systems is only possible from defined access points. This is only possible on Anexia's office premises or via a multi-layered, encrypted VPN dial-in by Anexia employees.*
- *The Client is given access to its systems by a secure, encrypted route, unless specified otherwise in the service description. The Client manages its access arrangements independently. Monitoring of the servers at system level (root / administrator access) is preferably carried out via key authentication.*
- *If passwords are used, they are generated according to very strict criteria (numbers, letters (upper and lower case), special characters, min. 15 characters).*
- *Access to systems is also possible locally in the computer center.*
- *All instances of access to the systems are logged and, at the request of the Client, are also stored externally.*
- *If Anexia does not have access to the Client's systems (e.g. unmanaged server), the Client is itself responsible for access.*

3. Access control to the data processing systems

Measures that ensure that the persons authorized to use a data processing system only have access to the data covered by their access rights and that personal data cannot be read, copied, modified or removed without authorization during processing and use or after storage:

Access to the systems is possible only via the defined access points of Anexia. All access is completely encrypted via SSH. Web-based administration systems are preferably encrypted by means of certified SSL so that the remote station can be verified. All access is logged and saved securely. These logs are accessible only to senior employees or managing directors/board members. Management of access is carried out by Anexia.

4. Transfer control

Measures that ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transfer, during transport or when it is saved on data carriers, and that it is possible to check and establish the points at which transfer of personal data is intended by means of data transfer equipment:

All systems are monitored and logged continuously. Senior employees monitor the work of all employees. Work is carried out on Anexia-certified systems only. All access is directly in the computer center, and other systems are controlled from there. It is not possible to access those systems from anywhere else. New employees are given non-critical work internally, in which it is not possible to view critical customer data. Only after a certain degree of trust and internal knowledge has been built up are employees given access to critical and confidential systems. If an employee leaves the company, all access is blocked centrally and generally applicable passwords are changed.

5. Input control

Measures to ensure that it is possible to check and establish in retrospect whether and by whom personal data has been entered into, modified in, or removed from data processing systems:

All systems are logged completely and are backed up on external systems with independent storage. Only senior employees have access to those external systems. The logs are saved for a minimum of three months.

6. Order control

Measures that ensure that personal data for which processing has been commissioned can only be processed according to the client's instructions.

Anexia works exclusively with permanent employees. External employees are not used for reasons of quality and security.

7. Availability control

Measures to ensure that personal data is protected against accidental damage or loss:

Anexia implements the following measures to ensure availability:

- *A power supply with high availability is ensured by a long battery life and/or a diesel generator. Servers with at least two power supply units are connected to different emergency power systems and also to different electrical fuses. As a result, failures of individual electrical circuits does not lead to the failure of the corresponding systems.*
- *Data backups are preferred, but at the request of the Client they are kept safe in a physically separate Anexia computer center. The Client's data is therefore fully available in the event of a disaster.*
- *Data backups of systems are set up in accordance with the specifications and coordination between the Anexia team and the Client's team. Data backups are usually carried out every day, with minimum storage of 4 weeks.*
- *Depending on the technical options, snapshots are also taken directly on the storage systems, which in turn are saved on an external technical platform.*
- *Backup data is saved on spindle-based systems (e.g. SATA). At the request of the client, a dedicated tape backup can be set up.*
- *Within the framework of the Client's commissioning of Anexia, the technical measures can be adapted as appropriate. The aim here should be to process personal data at all times according to the criticality of the data.*

8. Separation control

Measures to ensure that the data collected for different purposes can be processed separately:

Data is processed according to application. Anexia works in accordance with the corresponding specifications of the Client. The use of virtual LAN segments (VLAN) separates clients into different areas. Those VLANs are separated into public, private and storage VLANs. The way in which the VLANs are connected together is governed by the technical concept agreed between the Client and Anexia. The data of different Anexia clients is separated strictly logically so that none of the Anexia client data can be viewed by other clients.

§9 Information obligations, written form and choice of law

1. If the Client's data held by Anexia is at risk of distraint or seizure, at risk from insolvency or settlement proceedings or other events or measures relating to third parties, Anexia shall notify the Client immediately. Anexia shall immediately inform all parties with responsibility in this connection that the sovereignty and ownership of the data lie exclusively with the Client as the "controller" within the meaning of the General Data Protection Regulation.
2. Alterations and additions to this document and all of its component parts – including any undertakings from Anexia – must be agreed in writing, which includes electronic format (text form), and must contain an express reference to the fact that they constitute an alteration or addition to these conditions. This also applies to waiving this requirement of written form.
3. In the event of any contradictions, the provisions of this data protection document shall take precedence over the provisions of the contracts. Should individual parts of this document be invalid, this shall not affect the validity of the rest of the document.
4. Austrian law shall apply.

§10 Liability and compensation

The Client and Anexia accept liability in respect of data subjects in accordance with the provisions of Art. 82 GDPR. Other precedent liability and compensation provisions shall be agreed in the quotation or Master Services Agreement between the Client and Anexia.

Place, Date	Place, Date
Client	Anexia