alphaflow contract management (alphaflow-contract)
Data Processing Agreement

Between
You / the Customer

and
alphaflow GmbH
(hereinafter referred to as "alphaflow")

The Parties enter into this Data Processing Agreement (DPA) in connection with the General Terms and Conditions (GTC) governing the use of the services provided under the alphaflow Contract Management solution (technically: alphaflow-contract):

§ 1 Subject Matter and Duration of the Processing
The subject matter and duration of the processing are governed by the General Terms and Conditions (GTC).

§ 2 Purpose of the Processing
The activities performed by alphaflow serve the following agreed purposes:

- Support in the execution of contracts or assignments
- Sale or delivery of goods or provision of services
- Customer and business partner relationship management
- Ensuring proper and legally compliant accounting
- Invoicing for goods or services
- Maintenance and administration of employee data
- Documentation of working hours
- Payment of salaries and wages
- Planning and administration of training and development programs
- Documentation and definition of employee compensation and benefits
- Monitoring of operational facilities
- Ensuring access control and physical security
- Ensuring proper destruction of documents and data carriers
- Communication via electronic media
- Enabling contact with employees
- Documentation of employee appointments and schedules
- Access management for technical infrastructure (including telecommunications and network)
- Authorization management
- License management / software asset management
- Billing of telecommunications costs
- Maintenance and improvement of communication processes
- Quality assurance

§ 3 Categories of Personal Data

The following categories of personal data are subject to this Agreement:

- Master data (e.g. addresses)
- Personnel and identification numbers
- Customer behavior data
- Contract data
- User IDs
- Email addresses
- Passwords
- Access credentials

§ 4 Categories of Data Subjects

The following categories of data subjects are covered by this Agreement:

- Employees
- Trainees and interns
- Freelancers
- Shareholders and corporate officers
- Customers
- Prospective customers
- Suppliers and service providers
- Tenants
- Business partners
- External consultants

§ 5 General Provisions

This Data Processing Agreement (DPA) applies to all processing activities of personal data carried out by alphaflow under the scope of the General Terms and Conditions (GTC).

The Customer remains solely responsible under this DPA for ensuring compliance with all statutory provisions regarding the lawfulness of disclosing personal data to alphaflow, as well as for the legal basis of any personal data processing activities.

alphaflow shall process personal data strictly in accordance with the Customer's instructions, unless an exception under Article 28(3)(a) GDPR applies. Verbal instructions must be confirmed by the Customer in text form without undue delay.

Upon instruction from the Customer, alphaflow shall rectify or delete the personal data covered by the contract or restrict its processing (hereinafter referred to as "blocking").

alphaflow shall immediately inform the Customer if it believes that an instruction violates applicable data protection laws or this DPA. alphaflow may suspend execution of the instruction until the Customer confirms or modifies it in text form. alphaflow is entitled to reject the execution of any instruction that is clearly in violation of data protection law.

alphaflow ensures that all persons involved in the processing of personal data comply with the Customer's instructions and are contractually bound to confidentiality. The obligation of confidentiality shall continue after the termination of the processing activities.

§ 6 Technical and Organisational Measures (TOMs)
The Parties agree to implement appropriate technical and organisational measures pursuant to Article 32 GDPR to ensure an adequate level of protection for the data (hereinafter referred to as “Annex TOM”).
In the event of changes to Annex TOM, the agreed level of protection must not be reduced.

§ 7 Notification Obligations in the Event of Data Breaches
alphaflow shall notify the Customer without undue delay if it becomes aware of a personal data breach, as defined in Article 4(12) GDPR, relating to personal data processed by alphaflow within its area of responsibility, or if there is a concrete suspicion of such a breach. alphaflow and the Customer shall promptly take all necessary measures to remedy the data breach.

§ 8 Data Transfers to Third Countries
The transfer of data to a recipient in a third country outside the EU or EEA is permitted only in compliance with the conditions set forth in Articles 44 et seq. GDPR and requires the prior consent of the Customer in text form.

§ 9 Sub-processors
alphaflow may delegate the processing of personal data, in whole or in part, to other processors (hereinafter referred to as “sub-processors”).
The Customer may object to the engagement of a sub-processor for good cause by notifying alphaflow in text form. Good cause shall in particular exist where there are substantiated doubts as to the integrity of the sub-processor.
alphaflow shall enter into agreements with its sub-processors that impose the same data protection obligations as set out in this DPA.
Services used by alphaflow purely as ancillary services to support its business activities and which do not involve data processing within the scope of this DPA do not constitute sub-processing.

§ 10 Data Subject Rights and Assistance to the Customer
If a data subject asserts their rights under the GDPR against one of the Parties, that Party shall inform the other Party without undue delay.
alphaflow shall assist the Customer, to the extent possible, in responding to such requests and in complying with the obligations set forth in Articles 32 to 36 GDPR.

§ 11 Customer’s Audit and Inspection Rights
The Customer shall verify alphaflow’s technical and organisational measures prior to the commencement of data processing and on a regular basis thereafter. For this purpose, the Customer may, for example, request information from alphaflow, review existing audit reports from independent experts, certifications, or internal audits, or—after prior coordination and during normal business hours—conduct an on-site inspection of alphaflow’s technical and organisational measures, either personally or through a qualified third party, provided that such third party is not in a competitive relationship with alphaflow.
The Customer shall conduct audits only to the extent necessary and shall ensure that alphaflow’s business operations are not unreasonably disrupted.
alphaflow undertakes to provide the Customer, upon verbal or written request and within a reasonable period of time, with all information and documentation necessary for the inspection of its technical and organisational measures.
Upon request, alphaflow shall make available to the Customer a comprehensive and up-to-date data protection and security concept for the commissioned processing, including a list of persons authorized to access the data.

§ 12 Liability and Compensation

The Customer and alphaflow shall be liable to data subjects in accordance with the provisions of Article 82 GDPR. The Parties shall support each other in defending against any compensation claims asserted by data subjects.

§ 13 Term

The term of this DPA corresponds to the term of the General Terms and Conditions (GTC).

§ 14 Final Provisions

No verbal side agreements have been made. Any amendments or supplements to this DPA must be made in text form in order to be effective. This also applies to any changes to this clause.

If any provision of this DPA is or becomes invalid in whole or in part, the validity of the remaining provisions shall remain unaffected. In place of the invalid provision, the statutory regulation shall apply.

This DPA is governed by the laws of the Federal Republic of Germany, excluding the conflict of laws provisions. Article 3(3) and (4) of the Rome I Regulation (Regulation (EC) No. 593/2008) shall remain unaffected.

Annex: Technical and Organisational Measures (TOMs)
pursuant to Article 32 GDPR
The Parties agree on the following supplementary technical and organisational measures to be implemented by alphaflow under the Data Processing Agreement:

§ 15 Confidentiality (Article 32(1)(b) GDPR)

Physical Access Control
The following measures are in place to prevent unauthorized physical access to data processing facilities:

- Alarm system
- Video surveillance and recording using infrared systems
- Automated access control system with biometric fingerprint scanners
- Logging of all entries and exits
- Division of premises into three separately secured access zones
- Access exclusively via controlled entry systems (mantraps)
- 24/7 on-site personnel presence
- Separated and secured rooms for batteries, UPS, and power supply infrastructure
- Automated access control system using chip cards

Logical Access Control
The following measures are in place to prevent unauthorized access to data processing systems:

- Assignment of individual user rights and creation of user master records per user
- Definition of user profiles
- Granular permission control (profiles, roles, transactions, and objects)
- Password assignment
- Password policies (regular changes, minimum length, complexity requirements, etc.)
- Automatic lockout (e.g., due to incorrect password or inactivity timeout)
- Authentication via username and password
- Mapping of user profiles to IT systems
- Use of VPN technology for secure data transmission
- Deactivation/blocking of external interfaces (e.g., USB ports)
- Use of physical security locks
- Key management (issuance, return, and control)
- Identity checks at reception/security desk
- Visitor logging and registration
- Careful selection of cleaning staff
- Careful selection of security personnel
- Mandatory wearing of access badges
- Deployment of intrusion detection systems
- Use of antivirus software
- Encryption of data storage devices in laptops and notebooks
- Use of a hardware firewall
- Use of a software firewall

Data Access Control

The following measures ensure that unauthorized persons cannot access personal data:

- Access rights management concept
- Rights administration by a system administrator
- Regular review and update of access rights (especially in the event of employee departures or role changes)
- Limitation of the number of administrators to the minimum necessary
- Password policy including password length and periodic password changes
- Logging of access to applications, particularly during data entry, modification, and deletion
- Secure storage of data carriers
- Physical deletion of data carriers before reuse
- Proper destruction of data carriers in accordance with DIN 66399
- Use of shredders or certified service providers (preferably with a recognized data protection seal)
- Logging of data destruction activities
- Encryption of data carriers

Separation Control

The following measures ensure that data collected for different purposes is processed separately:

- Physical separation of storage on distinct systems or data carriers
- Logical software-based separation by means of multi-tenancy architecture
- Access rights and authorization concept
- Encryption of datasets processed for the same purpose
- Assignment of purpose-specific attributes/data fields and digital signatures to datasets
- Pseudonymized data: separation of the allocation file and its storage in a distinct and secured IT system
- Internal multi-client capability of the system
- Functional separation of production and test environments

Pseudonymisation (Article 32(1)(a) GDPR; Article 25(1) GDPR)

The processing of personal data is carried out in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and is subject to appropriate technical and organisational safeguards.

Pseudonymisation is implemented as follows: personal data is strictly separated from customer master data and transaction data. Where possible, personal data is encrypted during electronic transmission.

Integrity (Article 32(1)(b) GDPR)

Transmission Control

It is ensured that data cannot be read, copied, modified, deleted, or otherwise processed without authorization during transmission or while stored on data carriers, and that it is possible to verify which individuals or entities have accessed the data. The following measures have been implemented to ensure this:

- Use of VPN tunnels
- Logging systems
- Interface analysis
- Encryption of communication channels
- Encryption of physical data carriers during transport
- Data transmission using electronic signatures
- Secured transport procedures

Input Control

The following measures ensure that it is possible to verify who has entered, modified, or deleted data in data processing systems and at what time:

- Logging of data entries, modifications, and deletions
- Creation of an overview showing which applications can be used to enter, modify, or delete which data
- Traceability of data entries, modifications, and deletions through individual user accounts (not user groups)
- Retention of forms from which data has been transferred into automated processing systems
- Assignment of rights to enter, modify, and delete data based on an authorization concept

Availability and Resilience (Article 32(1)(b) GDPR)

The following measures are in place to ensure that data is protected against accidental destruction or loss and remains continuously available to the Customer:

- Redundant uninterruptible power supply (UPS) systems with up to 2,100 kVA capacity, using GreenPower UPS systems from Socomec
- Two independent power feeds via two sub-distribution panels in each rack
- Power supply of 10 kW or more per rack possible
- Emergency power supply via 1000 kVA diesel generators
- Direct proximity to a transformer substation
- Three-stage surge protection system: coarse protection in main distribution, medium/fine protection in sub-distributions, optional customer-level protection via proprietary power strips
- VESDA system for early smoke detection
- CO_2 fire extinguishers immediately available in all areas
- VdS-certified alarm systems
- Direct alerting of on-site technical personnel and external staff in case of incidents
- Server room climate control using a combination of direct and indirect free cooling
- Chilled water supply via energy-efficient units from Emerson Networks

- Air exchange through latest-generation systems by Weiss Klimatechnik
- Devices for monitoring temperature and humidity in server rooms
- Protected power strips in server rooms
- Intrusion alarm for unauthorized server room access
- Implementation of a comprehensive backup and recovery concept
- Regular testing of data restoration procedures
- Emergency response plan in place
- Secure off-site storage of backup data
- Robust data backup and recovery procedures in place
- Physical and logical data protection measures
- Backup procedures
- Disk mirroring using RAID systems
- Use of monitoring software
- Continuous monitoring of system functionality
- Use of CWDM technology for high bandwidth scalability
- Routing via modern Juniper routers
- Core switching via modern Cisco switches
- Uplinks optionally at 100 Mbit, 1 Gbit or 10 Gbit
- Redundant network connectivity via various carriers such as Tiscali International and Deutsche Telekom
- Peering connections at multiple exchange points, including DE-CIX, AMS-IX, KleyReX, VIX and NIX

Procedures for Regular Testing, Assessment and Evaluation (Article 32(1)(d) GDPR; Article 25(1) GDPR)

Data Protection Management

The following measures are in place to ensure an organizational structure that complies with the fundamental requirements of data protection law:

- alphaflow's data protection mission statement
- alphaflow's internal data protection policy
- Employee confidentiality agreements

Incident Management in Case of Data Protection Breaches

The following measures are implemented to ensure that appropriate notification processes are initiated in the event of a data protection incident:

- Breach notification procedure in accordance with Article 4(12) GDPR, including notifications to affected data subjects as required under Article 34 GDPR

Data Protection by Default (Article 25(2) GDPR)

Data protection-friendly default settings are applied both in the standardized configurations of systems and applications and during the setup of data processing operations. In this phase, specific functions and user rights are configured, data minimization principles are enforced by controlling the admissibility of inputs and input options, and the availability of functionalities is defined.

Additionally, the type and extent of personal reference or anonymization are determined (e.g. for selection, export, and evaluation functions, whether fixed, predefined, or customizable), as well as the availability of certain processing operations, functionalities, or logging features.

Order Control

The following measures ensure that data is processed exclusively in accordance with the Customer's instructions:

- Data Processing Agreement (DPA) including defined rights and obligations of the Parties
- Procedures for issuing and/or executing instructions
- Designation of contact persons and/or responsible personnel
- Monitoring and verification of instruction-based processing
- Employee confidentiality commitments
- Standardized contract management for monitoring sub-processors