Data Processing Addendum

Provisions on data protection and data security in contractual relationships

Preamble

This Data Processing Addendum (DPA) reflects the agreement of the parties with respect to the terms and conditions governing the processing of the Customer's personal data by a company of the proALPHA Group (hereinafter referred to as the "Contractor") under the existing contractual relationship between the parties. This DPA shall be incorporated by reference into the relevant contractual documents between the parties with legal effect as a schedule to the existing contract between the parties.

For existing Customers, the provision of this DPA by the Contractor to the Customer shall make it legally binding between the parties and constitute a legally effective amendment to the existing contractual agreement between the Parties.

The Customer has commissioned the Contractor to provide services from the proALPHA Group's product and service portfolio, in the course of which the Contractor will also process personal data on behalf of and in accordance with the instructions of the Customer:

To document the rights and obligations arising from the data processing relationship pursuant to the statutory obligations under Art. 28 GDPR (Processor), the Parties agree on the following.

1 Subject matter of the DPA, type, and purpose of processing

1) Consultation, implementation, supervision, support, maintenance and presentations of ERP Software proALPHA with all modules and the enhanced software offering, sold and implemented by proALPHA. The scope of the DPA, as well as the type and purpose of the processing are specified in **Annex 1.**

(2) In all other respects, the subject matter of the DPA is derived from the main contract and any amendments thereto to which reference is made here (hereinafter referred to as "Main Contract").

2 Type of personal data, categories of data subjects

(1) Type of data:

The type of personal data is shown in **Annex 1.**

(2) Persons involved:

The type data subjects is shown in **Annex 1.**

3 Term of DPA

The term of this DPA corresponds to the term of the Main Contract.

4 Responsibility and managerial authority

(1) The Customer is responsible for compliance with data protection legislation, specifically for the legality of data transfer to the Contractor and for the legality of data processing (Art. 4 no. 7 GDPR). The Contractor shall not use the data for any other purpose and, specifically, shall not be entitled to pass it on to third parties. Copies and duplicates shall not be created without the knowledge of the Customer. Exceptions apply only within the scope specified in paragraph 2.

(2) The Contractor shall process personal data only on the documented instructions of the Customer, unless otherwise required by EU law or the law of the member state to which the Contractor is subject. In the event of mandatory legal obligation, the Contractor shall immediately inform the Customer of the relevant legal requirements prior to processing.

(3) Verbal instructions must be confirmed immediately in writing or via e-mail (text form).

(3) If the Contractor is of the opinion that a directive violates data protection legislation, it shall immediately inform the Customer pursuant to Art. 28 para. 3 GDPR. The Contractor shall be entitled to suspend the execution of the directive until the corresponding directive has been confirmed or changed.

5 Confidentiality

To carry out the work, the Contractor shall only employ staff who have been obliged to maintain confidentiality in accordance with Art. 28 para. 3 lit. b GDPR and who have previously been familiarized with the relevant data protection provisions. The Contractor and any of its personnel who has access to personal data may process such data only in accordance with the directives of the Customer, including the powers granted in this DPA, unless processing is required by law.

6 Data security

(1) The Contractor shall take appropriate technical and organizational measures for the protection of personal data in accordance with Art. 28 para. 3 lit. c GDPR in conjunction with Art. 32 para. 1 GDPR in order to ensure secure processing. In doing so, the Contractor shall

- Ensure the continued confidentiality, integrity, availability and capacity of the systems and services connected to the processing.
- Ensure the capability to quickly restore availability of the personal data and access to it in the event of a physical or technical incident; and
- Maintain a process for the regular checking, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure secure processing.

In performing the above, the state of the art, implementation costs and type, scope and purposes of processing as well as the various probabilities of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be taken into account.

(2) The Parties agree on the specific data security measures set out in **Annex 3** to this DPA.

(3) The technical and organizational measures are subject to technological progress and further development. In this respect, the Contractor is permitted to implement alternative adequate measures. These alternative measures must not fall short of the security level of the defined measures. Significant amendments must be documented and communicated to the Customer via the Trustcenter.

7 Inclusion of additional sub-processors (subcontractors)

(1) In the context of this provision, subcontractors are processors commissioned by the Contractor whose services are directly related to the provision of the main service. This does not include ancillary services which the Contractor may use, for example, telecommunication services, post/transport services and cleaning. However, to ensure data protection and data security of the Customer's data, the Contractor is also obliged to conclude appropriate and lawful contractual agreements for outsourced ancillary services and to adopt reasonable monitoring measures.

(2) The Customer grants the Contractor the general authorization to engage sub-processors with regard to the processing of Customer Data. The subcontractors list **(Annex 2**) can be found under ***https://www.proalpha.com/de/trustcenter.*** The Contractor shall inform the Customer of any further engagement or replacement of subcontractors in a timely manner in advance by using the Trustcenter. Consent to subcontracting shall be deemed to have been given if the Customer does not object to the use of the subcontractor in question within 6 (six) weeks, commencing upon receipt of the information in the aforementioned sense. Any such objection shall only be permissible for justified reasons, such as insufficient reliability of the subcontractor.

If the Customer objects to the use of a subcontractor requested by the Contractor, the Contractor shall be entitled to terminate the main contract without notice and with immediate effect.

(3) A contractual agreement must be concluded with the subcontractor as per Art. 28, para. 3 and 4 GDPR which meets the requirements for confidentiality, data protection and data security of this agreement.

(4) The transmission of the Customer's personal data to the subcontractor and commencement of the subcontractor's activities are only permitted when all requirements for subcontracting are met.

(5) The processing of the data by the Contractor and the subcontractors approved by the Customer shall in principle take place exclusively in Member States of the European Union, Contracting States to the Agreement on the European Economic Area, and/or such countries for which a valid adequacy decision of the Commission applicable to the processing within the meaning of Article 45 para. 3 GDPR is available. The Contractor is nevertheless permitted to process Customer Data in accordance with the provisions of this agreement outside the EU/ EEA, provided that if subcontractors from a third country are involved, the Contractor shall inform the Customer in advance about the place of data processing and ensure that an adequate level of data protection is guaranteed by the subcontractor in question (for example, by establishing an agreement according to the EU standard data protection clauses). Section 7(2) of this DPA also applies to the commissioning of subcontractors in a third country.

(6) Any further outsourcing by the subcontractor requires the express consent of the Contractor (at least in text form). All contractual provisions in the contract chain must also be imposed on further subcontractors.

8 Support for the protection of data subject rights

(1) The Contractor shall be obliged to support the Customer with suitable technical and organizational measures in safeguarding the rights of the data subjects specified in Art. 12 to 22 GDPR (Art. 28 para. 3 lit. e GDPR). Specifically, the Contractor shall support the Customer in fulfilling claims of data subjects for deletion of their personal data in accordance with Art. 17 GDPR.

(2) The Contractor may only correct, delete or restrict the processing of personal data in accordance with the documented directive of the Customer (Art. 28 para. 3 S. lit. g GDPR). The Contractor may only provide information to third parties or the data subjects with the prior written consent of the Customer.

(3) If a data subject contacts the Contractor directly to assert their rights under Art. 12 to 22 GDPR, the Contractor shall immediately forward the request to the Customer.

9 Support for documentation and reporting obligations

(1) If the Contractor is legally obliged pursuant to Art. 37 GDPR, § 38 BDSG to appoint a data protection officer, the Contractor will on demand provide the Customer with the contact details of the data protection officer for the purpose of establishing direct contact.

(2) If the Contractor becomes aware of a breach of the protection of personal data, it must report this to the Customer without undue delay (Art. 28 para. 3 lit. f, Art. 33 para. 2 GDPR). The same applies if Contractor personnel act in violation of this DPA.

(3) After consultation with the Customer, the Contractor shall take the necessary measures to secure the data and to mitigate possible adverse consequences for the parties concerned without undue delay.

(4) The Contractor shall, to the best of its knowledge, support the Customer with its information obligations towards the responsible supervisory authorities as per Art. 33 GDPR and, if applicable, towards the data subject affected by the breach of the protection of personal data as per Art. 34 GDPR.

(5) The Contractor shall, to the best of its knowledge, support the Customer with the data protection adequacy evaluation as per Art. 35 GDPR and, if applicable, for any prior consultation by responsible supervisory authorities as per Art. 36 GDPR.

(6) The Contractor shall, without undue delay, inform the Customer of any checks and measures carried out by the supervisory authorities related to this DPA .

10 Termination of contract

(1) After completion of provision of the processing services, the Contractor shall either delete or return all personal data at the discretion of the Customer unless there is an obligation to save the personal data in accordance with EU Law or the law of the member states.

(2) Documentation that serves as proof of compliant data processing must be stored by the Contractor beyond the termination of the contract. The Contractor has the option to hand it over to the Customer when the contract ends.

11 Inspection rights of the Customer

(1) The Customer shall be entitled to regularly check the technical and organizational measures and compliance with this DPA and data protection legislation before and during the data processing.

(2) Should inspections by the Customer or an auditor commissioned by the Customer be necessary in individual cases, these shall be carried out during normal business hours without disrupting operations, following notification and taking into account a reasonable lead time (at least 72 time hours during working days). The Contractor may make inspections subject to prior notification with reasonable lead time and to the signing of a confidentiality agreement regarding the data of other customers. If the auditor commissioned by the Customer is in a direct competitive relationship with the Contractor, the Contractor shall have a right of objection against the auditor.

(3) The Contractor will, upon written request and within a reasonable period, provide the Customer with the information required to prove compliance with the obligations under this DPA and to prove the technical and organizational measures. For this purpose, the Contractor may also submit current attestations, reports, or report extracts from independent bodies (e.g. auditors, examiners, data protection officers, IT Security department, data protection auditors, quality auditors) or suitable certification by IT security or data protection audit. The Customer shall compensate the Contractor for the expenses incurred in providing such information.

12 Liability

The Customer and Contractor are liable towards third parties as per Art. 82 para. 1 GDPR for material or non-material loss or damage suffered by a person due to a breach of the GDPR. If both the Customer and the Contractor are responsible for such damage or loss pursuant to Art. 82 para. 2 GDPR, the Parties shall, as between themselves, share such liability in accordance with their respective share of responsibility. If, in such a case, a third party claims their losses entirely or predominantly from one party, that party may demand indemnification and holing harmless from the other party insofar as this corresponds to that other party;s share of responsibility.

13 Final provisions

(1) Data media and data records provided remain the property of the Customer.

(2) Should individual or several provisions of this DPA be invalid, this shall not affect the validity of the rest of this DPA. In the event that individual or several provisions are invalid, the Parties shall immediately replace the invalid provision with a provision that most closely corresponds to the invalid provision in terms of economics and data protection.

(3) In the case of a discrepancy between the Main Contract and this DPA, this DPA shall take precedence insofar as the discrepancy relates to the processing of personal data.

(4) The following annexes are an integral part of this agreement:

- Annex 1: Data Processing Specifications
- Annex 2: Approved Subcontractors ***https://www.proalpha.com/de/trustcenter***
- Annex 3: Technical and Organizational Measures

Annex 1

Data Processing Specifications (Art. 28 para. 3 S. 1 GDPR)

The Contractor provides a variety of services from the proALPHA Group's product and service portfolio for the Customer in the role of a general contractor. This Annex 1 contains the order-specific services and data processing within the meaning of Article 28 para. 3 S. 1 GDPR for the respective services provided by the Contractor.

The information applicable to this DPA is always based on the specific services that are the subject of the Main Contract concluded between the Parties and supplementary agreements.

proALPHA ERP Suite

The Contractor provides the Customer with a proALPHA ERP suite in which the Customer processes personal data. In the process of implementing the solution and in the case of support services, the Contractor will have access to the Customer's systems. Access to the Customer's personal data cannot be ruled out in this context.

Subject matter of the processing	**Type of data**	**Data subjects**	**Purpose**
-Remote- access as part of the implementation, development, support and maintenance of the systems	All data processed by the Customer within the proALPHA systems	All data subjects whose data is processed by the Customer within the proALPHA systems	Support in implementation, troubleshooting and support, maintenance and updating of the systems

proALPHA Business Cloud / Full Cloud Experience

The Contractor provides the Customer with servers for the operation of the proALPHA ERP Suite. The Contractor has no influence on the scope and type of the data processed by the Customer.

Subject matter of the processing	Type of data	Data subjects	Purpose
Provision of servers for external operation of the proALPHA ERP Suite	All data processed by the Customer within the proALPHA systems	All data subjects whose data is processed by the Customer within the proALPHA systems	Data Hosting

proALPHA Business Intelligence

The Contractor provides the Customer with a solution for visualization of processes and existing databases. The Customer alone decides on the type of data to be visualized.

Subject matter of the processing	Type of data	Data subjects	Purpose
Use of the "Qlik" visualization solution	All data that is part of a visualization order by the Customer.	All data subjects whose data are part of a visualization order by the Customer.	Data and process visualization
Use of the "Analyzer" visualization solution	All data that is part of a visualization order by the Customer.	All data subjects whose data are part of a visualization order by the Customer.	Data and process visualization

proALPHA Academy

The Customer uses the proALPHA Academy offering to provide users with system-specific specialist training and to document its execution.

Subject matter of the processing	Type of data	Data subjects	Purpose
Provision of an e-learning platform	Personal master data Learning progress	Users of the e-learning platform	Execution and documentation of professional training courses

L-Mobile CRM / Sales

The Contractor provides the Customer with a solution for operating a Customer Relationship Management (CRM) system.

Subject matter of the processing	Type of data	Data subjects	Purpose
Management of customer data in accordance with the Customer's wishes and specific use	Customer master data (e.g. name, address) Communication data (e.g. telephone number, e-mail address, fax number) Contact/Customer number Miscellaneous information processed by the Customer when using the system	Customers Contact person Other data subjects whose data the Customer processes when using the system	Transfer of relevant user information between the proALPHA ERP Suite and end devices of the Customer
Maintenance and servicing of the L-Mobile applications	Personnel master data Communication data Contract master data (contractual relationship, product or contractual interest) Customer history Log data Geo-coordinates Company data Sales data Material master data Customer master data Supplier master data Movement data (stock transfers, stock corrections, inventories) Types of data depending on the use of the system by the data controller	Employees of the Customer Clients of the Customer Interested parties of the Customer Suppliers Manufacturer's representatives Data subjects depending on the use of the system by the data controller	Setup, maintenance, troubleshooting for applications of L-mobile applications on the Customer's systems or on systems of clients of the Customer.

L-Mobile Warehouse

The Contractor shall provide the Customer with a solution for operating a warehouse interface in the area of production. This will be used to exchange relevant user data, default settings and granted privileges to end devices of the Customer.

Subject matter of the processing	Type of data	Data subjects	Purpose
Permissions management	User data (e.g. login information) Preferred language User privileges	User of end devices	Transfer of relevant user information between the proALPHA ERP Suite and end devices of the Customer
Maintenance and servicing of the L-Mobile applications	Personnel master data Communication data Contract master data (contractual relationship, product or contractual interest) Customer history Log data Geo-coordinates Company data Sales data Material master data Customer master data Supplier master data Movement data (stock transfers, stock corrections, inventories) Types of data depending on the use of the system by the data controller	Employees of the Customer Clients of the Customer Interested parties of the Customer Manufacturer's representatives' suppliers Data subjects depending on the use of the system by the data controller	Setup, maintenance, trouble-shooting for applications of L-mobile applications on the Customer's systems or on systems of clients of the Customer.

Curecomp

The Contractor operates various applications under the name "Clevercure", with regard to the use of which a contractual relationship exists between the Customer and the Contractor. These applications relate in particular to the "Supply Chain Management" category, but may also affect other areas in the Customer's company. Individual applications also include document management functionalities, whereby the type and scope of the use or discontinuation of the applications is at the discretion of the Customer and thus within the Customer's sphere of responsibility.

Subject matter of the processing	Type of data	Data subjects	Purpose
Operational modules: Exchange of personal data between procuring company and suppliers	User data (esp. name, e-mail address)	Employees of the Customer Employees of the Supplier	User management and provision of functionalities
Dispoengine, cleverconnect: Provision of interfaces between the systems of the Customer and the suppliers for the operation of the operational modules	User data (esp. name, e-mail address)	Employees of the Customer Employees of the Supplier	Automated communication between the systems of the Customer and the suppliers
Strategic modules: Establishment of data structures in accordance with the Customer's instructions; creation of workflows in accordance with the Customer's instructions	All data processed within the framework of data structures and workflows created by the Customer.	All persons whose data is processed within the framework of data structures and workflows created by the Customer.	Corresponds to the purpose specified by the Customer in each individual case.

Tisoware

The Contractor installs, implements, and maintains software systems from the product range of Tisoware Gesellschaft für Zeitwirtschaft GmbH for the Customer and provides deliverables and/or services in accordance with the contractual agreement of the existing Main Contract. These services and maintenance work can be carried out on site at the Customer's premises or by means of remote maintenance and customer support by the Contractor.

Subject matter of the processing	Type of data	Data subjects	Purpose
Access to Customer systems on site or via -remote- maintenance as part of the use of tisoware software	Personal master data (e.g. last name, first name, personnel number) Time recording data (e.g. coming, going, break times) Personnel scheduling data (e.g. shifts, shift models, vacation requests, absences) Personal data in connection with operating and machine data (start of order, details of order execution) Cafeteria data in connection with personal data (consumption) Access data (e.g. last name, first name, access time/place) Visitor data (e.g. last name, first name, company, visiting times) Travel data in connection with personal data Communication data (e.g. telephone/mail) Contract master data (contractual relationship, product and contractual interest) Customer history Contract billing and payment data	Employees of the Customer	Consulting, software installation and maintenance as well as support (incl. remote maintenance)

Böhme & Weihs

The Contractor provides services in the field of software maintenance, servicing, and updating for the "CASQ-it" and/or "MESQ-it" systems. In this context, the Contractor may obtain access to personal data and shall process such data exclusively on behalf of and in accordance with the instructions of the Customer. The scope and purpose of the data processing by the Contractor shall be drawn from the Main Contract (and the associated service description).

Subject matter of the processing	**Type of data**	**Data subjects**	**Purpose**
Access to Customer systems on site or via remote maintenance as part of the use of the "CASQ-it" and "MESQ-it" services	Personal master data Communication data (e.g. telephone, e-mail) Contract master data (contractual relationship, product or contractual interest) Customer history Contract billing and payment data Planning and controlling data Information disclosed (by third parties, e.g. credit agencies, public directories) Product data in Customer use	Clients of the Customer Interested parties of the Customer Employees of the Customer Suppliers of the Customer	Maintenance of the Customer's CAQ system, program changes, troubleshooting software errors, provision of updates

Corporate Planning

The Contractor provides training & consulting services or support services through support & maintenance (incl. remote maintenance) of systems in connection with the Contractor's software solution upon the Customer's request. In this context, access to and knowledge of personal data cannot be ruled out.

The Contractor furthermore provides a cloud infrastructure for the operation of the Contractor's software solution upon the Customer's request.

Subject matter of the processing	Type of data	Data subjects	Purpose
Training & consulting	Data processed by the Customer within the systems to which the Contractor has access within the scope of the service owed	Data subjects whose data is processed within the systems to which the Contractor has access within the scope of the service owed	Implementation of training and consulting measures with possible access to personal data of the Customer
Support and maintenance (incl. remote maintenance)	Data processed by the Customer within the systems to which the Contractor has access within the scope of the service owed	Data subjects whose data is processed within the systems to which the Contractor has access within the scope of the service owed	Implementation of support and maintenance for the use of the provided software according to service agreement with possible access to personal data of the customer
Corporate Planning Cloud	Data processed by the Customer within the CP Cloud.	Data subjects whose data is processed by the Customer within the CP Cloud	Provision of a cloud infrastructure

(Insiders) smart INVOICE

The Contractor provides a solution for digitizing incoming invoices. Here, essential content of incoming invoices is captured and all relevant invoice data is extracted by an algorithm. The data collected in this way can then be linked to further business processes. As a rule, no personal data is processed in this context. When using this function, however, it cannot be ruled out in individual cases that personal data of natural persons in the function of billers or bill recipients are processed and recorded by the system.

Subject matter of the processing	Type of data	Data subjects	Purpose
Analysis of invoice items in incoming invoices	Personal master data	Invoice issuer / recipient, insofar as they are natural persons	Recognition and extraction of relevant invoice fields for import into connected systems.

SAGE

The Contractor supports the Customer within the scope of product support for services from the product portfolio of Sage GmbH. When providing support services, there may be access to Customer systems. In this context, the possibility that the Contractor may become aware of the Customer's personal data cannot be ruled out.

Subject matter of the processing	Type of data	Data subjects	Purpose
Performance of support services including remote access and product updates	All data processed by the Customer within the SAGE systems	All data subjects whose data is processed by the Customer within the SAGE systems	Support with troubleshooting, product updates and other support services

Annex 2

Subcontractors list, see https://www.proalpha.com/de/trustcenter

Annex 3

Technical and organizational measures

The proALPHA Group follows a comprehensive site security concept. With the exception of site-specific access control, this is defined as binding for all with regard to further TOM.

it must be pointed out that in this description of the current status of the principle data protection measures, understandably, not all security measures can be disclosed in detail. Especially with regard to data protection and data security, the nondisclosure of confidential and detailed security descriptions is indispensable, since the protection of security measures against unauthorized disclosure is at least as important as the security measures themselves.

1 Confidentiality (Art. 32, para. 1 lit. b GDPR)

Access control

Unauthorized access shall be prevented, whereby the term refers to physical access.

- Alarm system
- Security locks
- Access authorization concept
- Manual locking system
- Locking system with code lock
- Key regulation / key book
- Automatic access control system (side entrances)
- Chip cards / transponder locking systems
- separate server rooms
- Data center located in Germany or the EU
- Data center ISO 27001-certified
- High-security access
- Alarm system with key and PIN
- Four-door system
- Careful selection of cleaning staff
- Careful selection of security staff
- Inspection of persons at gate / reception
- Visitor logging / guest book
- Mandatory wearing of employee / guest passes

Admission Control

Access by unauthorized persons to the IT systems or their unauthorized use must be prevented.

- Separate WiFi for guests
- Detailed user profiles
- Authentication with user + password
- Password rules
  - Use of individual passwords
  - Passwords with a minimum length
  - Limited number of failed attempts in a row
  - Password history
- Key regulation
- Encryption of mobile data media
- Autonomous remote maintenance
  - Integral part of the security concept of the pA Group
  - Access to internal server only via VPN
  - Central change of access privileges by IT administrators
  - Logging of server access at the user level

Access control

Unauthorized activities in DP systems outside the granted authorizations must be prevented.

- Detailed authorization concept
- Secure storage of data media
- Administration of user privileges by system administrators
- Number of administrators reduced to "bare minimum"
- Physical deletion of data media before their reuse
- Use of providers for file and data deletion (usually with option of certification)
- Use of intrusion detection systems
- Use of VPN technology
- Use of a hardware firewall
- Use of a software firewall
- Use of anti-virus software

Separation control

Data that has been collected for different purposes must also be processed separately.

- Definition of customer data rights
- Authorization concept that takes into account the separate processing of Customer data from the data of other customers
- Separation of production and test system
- Logical multiclient concept (through software)

2 Integrity (Art. 32, para. 1 lit. b GDPR)

Disclosure control

Aspects for transferring (transmitting) personal data are to be regulated:

- Electronic transfer, data transport, and checks thereof.
- Use of encrypted connections (e.g., VPN, HTTPS)
- Careful selection of transportation staff and vehicles
- Hardware disposal via shredding
- Privacy boxes for the disposal of confidential paper documents

Input control

The traceability or documentation of data management and maintenance must be ensured.

- Logging of input, modification and deletion of data
- The following activities are logged: booting and shutdown of central computers (e.g., servers and firewalls)
- Assignment of privileges for entering, modifying and deleting data on the basis of an authorization concept
- Storage of forms from which data were adopted for automated processing
- Tracing of entry, modification and deletion of data by individual user names (not user groups)

3 Availability and resilience (Art. 32 para. 1 lit. b GDPR)

Availability control and resilience

The data shall be protected against accidental destruction or loss. Systems must have the capability to handle risk-related changes and show failure tolerance and the ability to compensate for failures.

- Air-conditioning system in server rooms
- Fire and smoke alarms
- Fire extinguishers in server rooms
- Testing of data recovery
- Safety socket bars in server rooms
- Server rooms are not below sanitary installations
- Backup & recovery concept
- Uninterrupted power supply (UPS)
- Storage of backup at a safe, different location
- Devices for monitoring the temperature and humidity in server rooms / IT rooms

4 Process for regular testing, assessing and evaluating (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

Control procedures

A procedure for the regular review, assessment, and evaluation of the effectiveness of the data security measures must be implemented.

- Code of Conduct available
- Report new/changed data processing procedures to the data protection officer
- Data protection management available
- Data protection concept available

5 Home Working Regulations

The proALPHA Group enables its employees to perform work via remote access. Measures have been taken to meet the security standard of the general security concept. This applies where applicable and is supplemented by the following measures.

The measures are divided into **technical measures** that affect access to the system and **organizational measures** that affect how the respective employee handles data at their home workstation.

Technical measures

The measures below represent the additional measures taken. For access to the system proALPHA use the following measures

- Access exclusively via official business devices
- End devices are subject to regular updates on the IT side
- Applications may only be installed after consulting the whitelist available for this purpose. Applications not approved by IT must not be installed
- Access is done exclusively through an encrypted connection
- Windows
  - endpoint security
  - antivirus software
  - system data encryption
  - proxy for domain filtering
- iOS clients
  - Managed by Airwatch MDM/Workspace One
  - Control over the device with the possibility of remote "wipe" or "lock"
  - Complete encryption of the device
  - Protected by six-digit passcode
  - Restriction policy
    - Untrusted certificates cannot be accepted manually
    - No diagnostic data to Apple
    - User cannot trust third party apps manually

Organizational measures

In organizational terms, various supplementary agreements and internal guidelines have been issued to supplement the measures in the general TOM.

This includes, but is not limited to, the following regulations and obligations:

- Right of access to and inspection of the workplace by internal appointed inspectors (e.g. occupational safety specialist or company data protection officer)
- Obligation to internal directive on the use of technical equipment
- Obligation to protect access to work equipment by not authorized personnel
- Prohibition against use of personal technical equipment (excluding WiFi, peripheral devices like keyboard and mouse without driver installation)
- Obligation to keep confidential physical documents under lock and key
- Obligation to confidentiality / secrecy
- Obligation to notify on change of residence