Data Processing Addendum

Provisions on data protection and data security in contractual relationships

Proalpha

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 (hereinafter referred to as the "Customer") personal data by a company of the Proalpha Group (hereinafter referred to as the "Contractor") under the contractual relationship existing between the parties. The agreement on data processing shall be incorporated by reference in respective contractual documents between the parties with legal effect as an annex to the contractual relationship existing between the parties.

For existing Customers, the provision of this Agreement by the Contractor to the Customer shall constitute a legally effective amendment to the existing contractual agreement as well as be legally binding between the Parties.

The Customer has commissioned the Contractor to provide services from the Proalpha Group's product and service portfolio. In this process, the Contractor will also process personal data on behalf of and in accordance with the instructions of the Customer.

To substantiate the rights and obligations arising from the contract processing relationship as per the statutory obligation from Art. 28 GDPR, the Parties agree on the following.

1 Subject of the contract, 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, which is sold and implemented by Proalpha. The subject of the contract, 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 contract results from the Main Contract and the follow-up contracts concluded for the period of active maintenance 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 data subjects are shown in **Annex 1.**

3 Duration of contract

The duration of this contract (term) corresponds to the duration of the main contract.

4 Responsibility and managerial authority

(1) The Customer is responsible for compliance with data protection provisions, 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 Union law or the law of the member state to which the Contractor is subject. In the event of an alternative obligation, the Contractor shall immediately inform the Customer of the relevant legal requirements prior to processing.

(3) If the Contractor is of the opinion that a directive violates data protection regulations, they shall immediately inform the Customer pursuant to Art. 28 para. 3 S. 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 (2) lit. b GDPR and who have previously been familiarized with the relevant data protection provisions. The Contractor and any person subject to the Contractor 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 Contract, unless processing is required by law.

6 Data security

(1) The Contractor shall take suitable technological and organizational measures for the appropriate 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 permanent 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 also
- maintain a process for the regular checking, assessment and evaluation of the effectiveness of the technological and organizational measures to ensure processing security.

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 defined in **Annex 3** to this agreement.

(3) The technological and organizational measures are subject to technological advancements 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 trust center.

7 Inclusion of additional 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 monitoring measures.

(2) The customer hereby grants the contractor general authorization to subcontract: The list **(Appendix 2)** can be found in the trust center at https://www.proalpha.com/de/trustcenter. The contractor has to inform the customer about the planned use of another subcontractor or the replacement of an existing subcontractor in advance via the trust center. Consent to subcontract shall be deemed to have been given if the contracting entity does not object to the use of the subcontractor concerned within 6 (six) weeks, starting with the receipt of the information referred to above. Such an objection is only valid for legitimate reasons, such as insufficient reliability of the subcontractor.

If the customer objects to the use of a subcontractor requested by the supplier, the supplier is entitled to terminate the main contract without giving notice and with immediate effect.

(3) A contractual agreement as per Art. 28, para. 3 and 4 GDPR shall be concluded with the subcontractor, which meets the requirements for confidentiality, data protection and data security of this agreement. The Customer shall be entitled to view the Contractor's contracts with subcontractors and to request that the Contractor provide a copy of these contracts.

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

(5) The processing of the data by the data processor and the sub-service providers 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. Any processing in another country ("Unsafe Third Country") requires the prior written approval of the Customer and, moreover, may only take place if the legal requirements for data transfers to Unsafe Third Countries under the applicable data protection laws are met.

Insofar as the Customer reasonably deems this necessary, the Contractor shall support them with the information available to them in the evaluation and legally compliant structuring of the data processing relationship.

(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 the other subcontractors.

(7) The subcontractors approved at the time of conclusion of the contract are shown in **Annex 2.**

8 Support for the protection of data subject rights

(1) The Contractor shall be obliged to support the Customer with suitable technological and organizational measures in safeguarding the rights of the data subjects specified in Art. 12 to 22 GDPR (Art. 28 para. 3 S. 2 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. 2 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 shall provide the Customer with the contact details of the data protection officer for the purpose of establishing direct contact. The Customer must be notified immediately if the data protection officer is changed.

(2) If the Contractor becomes aware of a breach of the protection of personal data, they shall immediately report this to the Customer (Art. 28 para. 3 lit. f, Art. 33 para. 2 GDPR). The same applies if persons employed by the Contractor act in violation of this agreement.

(3) After consultation with the Customer, the Contractor shall immediately take the necessary measures to secure the data and to mitigate possible adverse consequences for the parties concerned.

(4) The Contractor shall support the Customer by disclosing all information available to them as per Art. 33 GDPR for fulfillment of the information obligations towards the responsible supervisory authorities 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 support the Customer by disclosing all information available to them as per Art. 35 GDPR for the data protection adequacy decision and, if applicable, for any prior consultation by responsible supervisory authorities as per Art. 36 GDPR.

(6) The Contractor shall inform the Customer immediately of any checks and measures carried out by the supervisory authorities if they refer to this contract.

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 Union Law or the law of the member states.

(2) Without further demand, the Contractor shall provide dated written evidence to the Customer that they have returned all data media and other documentation to the Customer or destroyed or deleted them in compliance with data protection regulations and thus that they have not retained any Customer data.

(3) Documentation that serves as proof of orderly and contractual data processing must be stored by the Contractor beyond the termination of the contract. They have the option to hand it over to the Customer when the contract ends.

11 Control rights of the Customer

(1) The Customer shall be entitled to regularly check the technological and organizational measures and compliance with this agreement and data protection legislation specifications before and during the processing services. For this purpose, the Customer or an authorized person may inspect the Contractor's data processing systems and data processing programs.

(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, working days). The Contractor may make them 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 undertakes to provide the Customer, upon written request and within a reasonable period of time, with the information required to prove compliance with the obligations under this data processing agreement 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 this information.

12 Liability

The Customer and Contractor are liable in an external relationship 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 be liable in an internal relationship for this damage in accordance with their share of responsibility. If, in such a case, a person entirely or predominantly claims a party for damages, this party may demand exemption or indemnification from the other party insofar as this corresponds to its 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 agreement be invalid, this shall not affect the validity of the rest of this agreement. 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 agreement, this agreement 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 at https://www.proalpha.com/en/trustcenter
- Annex 3: Technological 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 function 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 agreement is always based on the specific services that are the content of the main contract concluded between the Parties and supplementary agreements.

Proalpha ERP

The Contractor shall provide the Customer with a software 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 excluded 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 / Proalpha Cloud Platform Services

The Contractor shall provide the Customer with servers and services for Proalpha and Proalpha group company products. 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 and maintainance of servers and services for Proalpha and group company products.	All data processed by the Customer within the cloud system	All data subjects whose data is processed by the Customer within the cloud system	Operation of Proalpha cloud solution for the contractor

Proalpha Business Intelligence and NEMO

The Contractor shall provide 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
NEMO modules: Building of data structures according to the instruction of the customer; anonymization of data records for the purpose of analysis according to the instruction of the customer	All data that is processed in the context of the data structures provided by the Customer.	Employees of the Customer.	Configuration of analysis factors. Corresponds to the purpose defined by the Customer in the individual case.

Proalpha Academy

The Customer shall use 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 Customer shall provide the Contractor 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 Customer shall provide the Contractor 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, troubleshooting for applications of L-mobile applications on the Customer's systems or on systems of clients of the Customer.

DIG

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, clever-connect: 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 / Atoria – the people software GmbH

The Contractor shall install, implement, and maintain software systems from the product range of Atoria – the people software GmbHfor the Customer and shall provide 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 shall provide services in the field of software maintenance, servicing, and updating for the "CASQ-it" and/or "MESQ-it" systems provided in each case. 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 shall provide 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 excluded.

The Contractor shall furthermore provide 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 shall provide 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 shall support 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 excluded.

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

Empolis

The Contractor provides a cloud solution for building a central knowledge base under the name "Proalpha connected knowledge". The use of this AI-based knowledge management system allows data and documents from various systems of the host to be easily searched in a uniform environment. The Customer defines the connected data sources, e.g. Proalpha DMS, local file shares, sharepoint areas, data from superseded legacy systems. In addition, the cloud solution supports the easy creation and exchange of expertise.

Subject matter of the processing	Type of data	Data subjects	Purpose
Creating and managing user accounts and creating expert communities.	Account and access data	Users of the system that are defined by the authorized agents of the remitter.	User management and provision of functionalities of the knowledge management system by authorized representatives of the Customer.
Indexing and semantic linking of documents and knowledge articles	Documents and records from connected systems of the Contractor	Employees of the Customer Customers of the Customer Prospects of the Customer Suppliers of the Customer	Easy access to documented knowledge within the company

Annex 2

Approved Subcontractors

The list of approved subcontractors is always up-to-date found on the following link:

https://www.proalpha.com/de/trustcenter

Annex 3

Technological 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.

In this description of the current status of the basic data protection measures, it must be pointed out that, 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 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 spatial 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
- Redundant server rooms
- Data center in Kaiserslautern
- 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 of unauthorized persons to the IT systems or their unauthorized use should be prevented

- Separate WiFi for guests
  - Central and separate Internet access via Weilerbach, which is encapsulated through VLAN and Multi-SSID.
  - All APs around the world are managed by means of WiFi controllers.
  - The guest WiFi can only be accessed with a password and WPA2.
  - The password is changed on a weekly basis.
  - Each WiFi user must comply with the internal terms of use.
- 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
- Data center in Kaiserslautern
  - ISO 27001-certified
- 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 database 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 company separation (through software)
- Physically separate storage on separate systems or data media

Pseudonymization

The processing of personal data in such a way that the data cannot be assigned to a specific data subject without the involvement of additional information, provided that this additional information is stored separately and is governed by corresponding technological and organizational measures;

- Data records have been analyzed and pseudonymized on the basis of these results.
- Separation of assignment file and storage on a separate, secured IT system

Technical measures

The measures below represent the additional measures taken. For access to the system within the framework of an existing VPN connection, reference is made to the general TOM applicable for this purpose.

- Access exclusively via official 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 VPN connection
- Windows clients
  - Checkpoint endpoint security client
    - Access to VPN tunnel via TAN created via software or hardware token
    - Local firewall configured by Team Infrastructure
  - Trend Micro antivirus software
  - Encrypted system with startup PIN (BitLocker)
  - ZScaler 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 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 third parties
- Prohibition against use of personal technical equipment (excluding WiFi, peripheral devices like keyboard and mouse without driver installation)
- Obligation to keep official documents under lock and key
- Obligation to confidentiality / secrecy
- Obligation to notify on change of residence

Home Office

The Proalpha Group enables its employees to perform incidental 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 office.

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 encoded VPN connections
- Careful selection of transportation staff and vehicles
- Shredder for the secure destruction of data
- 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)
- Data center in Kaiserslautern
  - ISO 27001-certified
- Storage of backup at a safe, external 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