

Data Processing Agreement

Provisions on Data Protection and Data Security in
Contractual Relationships

Preamble

The customer (hereinafter referred to as "Customer") has commissioned the Proalpha GmbH (hereinafter referred to as "Contractor") to provide services from the product and service portfolio of the Proalpha Group. In this context, the Contractor shall also process personal data on behalf of and in accordance with the instructions of the Customer.

This Data Processing Agreement specifies the rights and obligations of the Parties with regard to the processing of the Customer's personal data by the Contractor within the framework of the contractual relationship between the Parties. By being incorporated by reference into the respective contract documents between the Parties, it becomes a binding annex and thereby gains legal effect. For existing customers, the provision of this Data Processing Agreement by the Contractor to the Customer constitutes a legally effective amendment to the contractual relationship between the Parties and is thus legally binding between them.

To substantiate the rights and obligations arising from the contract processing relationship in accordance with the legal requirements of Art. 28 GDPR, the Parties enter into the following Data Processing Agreement.

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. This notwithstanding, the subject of the Contract is defined by the offer, the general terms and conditions, and all other documents referenced therein (hereinafter referred to as "Agreement").

2 Type of Personal Data, Categories of Affected Persons

(1) Type of data:

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

(2) Data subjects:

The data subjects are shown in **Annex 1**.

3 Duration of Contract

The duration of this Contract corresponds to the term of the Agreement.

4 Responsibility and Authority to Issue Instructions

(1) The Customer is responsible for compliance with data protection regulations, in particular for the lawful transfer of data to the Contractor and for the lawful processing of the data (Art. 4 No. 7 GDPR). The Contractor shall not use the data for any other purposes and shall, in particular, not be authorized to disclose it to third parties. Copies and duplicates shall not be created without the knowledge of the Customer. Exceptions apply only to the extent specified in paragraph 2.

(2) The Contractor shall process personal data only on documented instructions from the Customer, unless required to do so by Union law or law of the Member State to which the Contractor is subject. In the event of an alternative obligation, the Contractor shall promptly inform the Customer of the relevant legal requirements prior to processing.

(3) The Customer shall promptly confirm oral instructions in writing or by email (in text form).

(4) If the Contractor is of the opinion that an instruction violates data protection regulations, it shall promptly inform the Customer in accordance with Art. 28 para. 3 S. 3 GDPR. Until the instruction in question is confirmed or amended, the Contractor shall be entitled to suspend its execution.

5 Confidentiality

The Contractor shall engage only employees for the performance of the work who have been committed to confidentiality in accordance with Art. 28 para. 3 (2) lit. b GDPR and who have been informed of the data protection provisions relevant to their duties. The Contractor and any person acting under the Contractor's authority who has access to personal data may process such data only in accordance with the Customer's instructions, including the authorizations granted in this Agreement, unless they are legally obligated to process the data.

6 Data Security

(1) The Contractor shall take suitable technical 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. To this end, the Contractor shall

- ensure the ongoing confidentiality, integrity, availability and resilience of the systems and services related to processing;
- ensure the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident; and
- maintain a procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to ensure processing security.

In doing so, due consideration shall be given to the state of the art, the cost of implementation, and the nature, scope, context and purposes of processing, as well as the varying likelihood and severity of risks to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR.

(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 technical advancements and further development. To that extent, the Contractor is permitted to implement alternative adequate measures. These alternative measures must not provide a lower level of security than the defined

measures. Significant amendments must be documented and communicated to the Customer via the Trust Center.

7 Inclusion of Additional Processors (Subcontractors)

(1) Subcontractors within the meaning of this provision are processors engaged by the Contractor whose services directly relate to the performance of the primary service. This does not include ancillary services used by the Contractor, such as telecommunications services, postal or transport services, and cleaning services. However, the Contractor is obligated to implement appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security for the Customer's data, even in the case of outsourced ancillary services.

(2) The Contractor hereby grants the Customer general authorization to engage subcontractors: The list (**Annex 2**) can be found in the Trust Center under <https://www.Proalpha.com/en/trustcenter>. The Contractor shall inform the Customer with sufficient prior notice about the planned engagement of an additional subcontractor or the replacement of an existing subcontractor. The information is provided via the Customer Portal and the Trust Center. Consent to subcontracting shall be deemed granted if the Customer does not object to the engagement of the respective subcontractor within six (6) weeks of receiving the corresponding information as described above. Any such objection shall only be permissible for justified reasons, such as insufficient reliability of the subcontractor.

If the Customer exercises its right to object to the use of a subcontractor designated by the Contractor, the Parties shall first seek to reach an amicable solution. If no solution is reached within a reasonable period of time and the use of the subcontractor is essential for the performance of the services, the Contractor shall be entitled to terminate the Agreement for cause 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 DPA.

(4) The transmission of the Customer's personal data to the subcontractor and the commencement of the subcontractor's activities shall only be permitted once all requirements for subcontracting have been met.

(5) The processing of data by the processor and the subcontractors approved by the controller shall generally take place in Member States of the European Union, in Contracting States of the Agreement on the European Economic Area, and/or in countries for which a valid adequacy decision by the Commission applicable to the processing pursuant to Article 45 para. 3 GDPR exists. The processor is permitted to process Customer data outside the EU/EEA in compliance with the provisions of this Agreement, provided that the processor informs the Customer in advance about the location of the data processing and ensures that an adequate level of data protection is guaranteed by the respective subcontractor (e.g., through the conclusion of an agreement based on the EU Standard Contractual Clauses). The provision in 7 (2) of this DPA shall therefore also apply to the engagement of subcontractors in third countries.

(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.

8 Support for the Protection of Data Subject Rights

(1) The Contractor shall be obligated 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 S. 2 lit. e GDPR). In particular, the Contractor shall support the Customer in fulfilling requests of data subjects for the deletion of their personal data in accordance with Art. 17 GDPR.

(2) The Contractor may rectify, delete or restrict the processing of personal data only on documented instructions from 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 its rights under Art. 12 to 22 GDPR, the Contractor shall promptly forward the request to the Customer.

9 Support with Documentation and Reporting Obligations

- (1) If the Contractor is legally obliged to appoint a data protection officer pursuant to Art. 37 GDPR and Section 38 BDSG, the Contractor shall provide the Customer with the contact details of the data protection officer upon request for the purpose of establishing direct contact.
- (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 DPA.
- (3) After consultation with the Customer, the Contractor shall promptly 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 it in fulfilling the information obligations toward the competent supervisory authority pursuant to Art. 33 GDPR and, where applicable, toward the data subjects affected by the personal data breach pursuant to Art. 34 GDPR.
- (5) The Contractor shall support the Customer by disclosing all information available to it in carrying out the data protection impact assessment pursuant to Art. 35 GDPR and, if applicable, for any prior consultation by responsible supervisory authorities as per Art. 36 GDPR.
- (6) The Contractor shall inform the Customer promptly of any inspections and measures undertaken by the supervisory authority, insofar as they relate to this Agreement.

10 Termination of Agreement

- (1) Upon completion 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 retain the personal data under Union or Member State law.
- (2) Documentation serving as evidence of contractually compliant and proper data processing shall be retained by the Contractor beyond the termination of the Agreement. The Contractor may, for its discharge, hand over such documentation to the Customer upon termination of the Agreement.

11 Control Rights of the Customer

(1) The Customer shall be entitled to verify the technical and organizational measures, as well as compliance with this DPA and data protection regulations, prior to the commencement of the processing services and on a regular basis thereafter.

(2) Should inspections by the Customer or an auditor appointed by the Customer be required in individual cases, they shall be conducted during regular business hours without disrupting operations, following prior notice and with due consideration of a reasonable lead time (at least 72 business hours). The Contractor may make such inspections contingent upon prior notice with a reasonable lead time and the signing of a confidentiality agreement with respect to other customers' data. If the auditor appointed by the Customer is in direct competition with the Contractor, the Contractor shall have the right to object to their involvement.

(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 verify the technical and organizational measures. For this purpose, the Contractor may also submit current attestations, reports, or excerpts from reports issued by independent bodies (e.g., auditors, examiners, data protection officers, IT security department, data protection auditors, quality auditors) or provide appropriate certification from an IT security or data protection audit. The Customer shall reimburse the Contractor for the effort incurred in providing the requested information.

12 Liability

The Customer and Contractor shall be liable to third parties in accordance with Art. 82 para. 1 GDPR for material or non-material damage suffered by a person as a result of an infringement of the GDPR. If both the Customer and the Contractor are responsible for such damage in accordance with Art. 82 para. 2 GDPR, the Parties shall be liable internally for the damage in proportion to their respective share of responsibility. If, in such a case, a person claims compensation in full or in large part from one Party, that Party may request indemnification or hold harmless from the other Party to the extent corresponding to the latter's share of responsibility.

13 Final Provisions

(1) Provided data carriers and datasets remain the property of the Customer.

(2) If any provision of this DPA is or becomes invalid, the validity of the remaining provisions shall not be affected. In the event that one or more provisions are found to be invalid, the Parties shall promptly replace the invalid provision with one that most closely reflects its economic intent and data protection requirements.

(3) In the case of a discrepancy between the Main Agreement 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 DPA:

- Annex 1: Data Processing Specifications
- Annex 2: Approved Subcontractors under <https://www.proalpha.com/en/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 function of a general contractor. This Annex 1 contains the contract-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 content of the Main Agreement 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 course of implementing the solution and in the event 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 / Proalpha Cloud Platform Services

The Contractor shall provide the Customer with servers and services for Proalpha and the products of the Proalpha Group. The Contractor shall have 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 maintenance of servers and services for Proalpha and the products of the Proalpha Group.	All data processed by the Customer within the Cloud system	All data subjects whose data is processed by the Customer within the Cloud systems	Operation of the Proalpha Cloud solution on behalf of 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 shall decide 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: Establishment of data structures in accordance with the Customer's instructions; anonymization of datasets for analysis purposes in accordance with the Customer's instructions	All data processed within the data structures provided by the Customer.	Employees of the Customer	Configuration of analysis factors. Corresponds to the purpose specified by the Customer in each 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 e-learning offerings	Personal master data Learning progress	Users of the e-learning offering	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)	Customers	Transfer of relevant user information between the Proalpha ERP Suite and end devices of the Customer
	Communication data (e.g. telephone number, email address, fax number)	Contact persons	
	Contact/Customer number	Other data subjects whose data the Customer processes when using the system	
	Other information processed by the Customer when using the system		
Maintenance and servicing of the L-Mobile applications	Personnel Master Files	Employees of the Customer	Setup, maintenance, troubleshooting for applications of L-mobile applications on the Customer's systems or on systems of clients of the Customer.
	Communication data	Clients of the Customer	
	Contract master data (contractual relationship, product or contractual interest)	Interested parties of the Customer	
	Customer history		
	Log data	Suppliers	
	Geo-coordinates	Manufacturer's representatives	
	Company data		
	Sales data		
	Material master data	Data subjects depending on the use of the system by the body responsible	
	Customer master files		
	Supplier master files		
	Movement data (stock transfers, stock corrections, inventories)		
Types of data depending on the use of the system by the responsible body			

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 files 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 files Supplier master files Movement data (stock transfers, stock corrections, inventories) Types of data depending on the use of the system by the responsible body	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 body responsible	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 are mainly associated with the "Supply Chain Management" category, but may also affect other parts of the Customer's organization. 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, email 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, email 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 GmbH for the Customer and shall provide deliverables and/or services in accordance with the contractual agreement of the existing Main Agreement. 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 tracking data (e.g. arrival, departure, break times) Personnel scheduling data (e.g. shifts, shift models, vacation requests, absences) Personal data in connection with operating and machine data (start of contract, details of contract 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	Clients of the Customer	Maintenance of the Customer's CAQ system, program changes, troubleshooting software errors, provision of updates
	Communication data (e.g. telephone, email)	Interested parties of the Customer	
	Contract master data (contractual relationship, product or contractual interest)	Employees of the Customer	
	Customer history	Suppliers of the Customer	
	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		

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	Provision of support and maintenance services for the provided software in accordance with the Service Level 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. Access to Customer systems might be required for providing support services. 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 under the name "Proalpha connected knowledge" for building a centralized knowledge base. This AI-powered knowledge management system allows the Customer to easily search data and documents from multiple systems within a single environment. The Customer specifies the connected data sources, such as Proalpha DMS, local file shares, Share-Point sites, or data from decommissioned legacy systems. Furthermore, the Cloud solution simplifies the creation and exchange of expert knowledge.

Subject matter of the processing	Type of data	Data subjects	Purpose
Creation and management of user accounts and establishment of expert communities.	Account and access data	Users of the system as defined by authorized agents of the Customer.	User administration and provision of the knowledge management system's functionalities by authorized agents of the Customer.
Indexing and semantic linking of documents and knowledge articles	Documents and datasets from the Customer's connected systems	Employees of the Customer Clients of the Customer Interested parties of the Customer Suppliers of the Customer	Easy access to documented knowledge within the company.

Gedys CXM/CRM (on-premises service)

The Contractor shall provide the Customer with software in which the Customer processes personal data. In the course of implementing the solution and in the event 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. Depending on the specific use and customer configuration, the subject

matter of the processing is determined, and the data processed are those that the Customer maps within the system.

Subject matter of the processing	Type of data	Data subjects	Purpose
Provision and implementation of the Gedys CXM/CRM system within the Customer's internal corporate environment for the management and analysis of customer data	All data processed by the Customer in the context of using the CXM/CRM software, in particular:	All data subjects whose data are processed by the Customer within the Gedys systems, in particular:	Support in implementation, configuration, programming, troubleshooting and support, maintenance and updating of the system
Access in the context of support, maintenance, system configurations and updates, as well as customizations of CXM/CRM software	Customer/supplier/employee master data Communication data Contact/customer number Contract master data Customer history Contract billing and payment data Sales data	Customers Partners Prospects Suppliers Contact persons of the customers/partners/prospects/suppliers Employees	

Gedys CXM/CRM (SaaS/hosting service)

The Contractor shall provide the Customer with software in which the Customer processes personal data. In the course of implementing the solution and in the event 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. Depending on the specific use and customer configuration, the subject matter of the processing is determined, and the data processed are those that the Customer maps within the system.

Subject matter of the processing	Type of data	Data subjects	Purpose
Implementation and operation of Gedys CXM/CRM in the cloud: provision of the cloud-based solution including data storage and backup.	All data processed by the Customer in the context of using the CXM/CRM software, in particular:	All data subjects whose data are processed by the Customer within the Gedys systems, in particular:	Support in implementation, configuration, programming, troubleshooting and support, maintenance and updating of the system
Access in the context of support, maintenance, system configurations and updates, as well as customizations of the CXM/CRM software, incl. revision management	Customer/supplier/employee master data Communication data Contact/customer number Contract master data Customer history	Customers Partners Prospects Suppliers Contact persons of the customers/partners/prospects/suppliers	
Interface management	Contract billing and payment data	Employees	
Reporting and monitoring	Sales data		
Access control and authentication			

Annex 2

List of subcontractors, see <https://www.Proalpha.com/en/trustcenter>

Annex 3

1 Technical and Organizational Measures

The Proalpha Group pursues a comprehensive site security concept. With the exception of site-specific access control, this concept shall be binding for everyone with regard to the other TOMs.

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.

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

2.1 Access control

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

- Security locks
- Access authorization concept / Zone protection concept
- Manual locking system
- Locking system with code lock
- Chip card locking system
- Data centers located in Germany or within the EU
- Data centers certified according to ISO 27001
- Separate IT distribution rooms
- Inspection of persons at gate / reception
- Visitor logging / guest book

2.2 System access control

Unauthorized access to IT systems and their unauthorized use must be prevented.

- Security Operation Center with 24/7 SIEM available
- Authorization concept: Privileged Access Management (PAM) based on the need-to-use and need-to-know principles
- Separate guest Wi-Fi
- Personalized user profiles
- Authentication with username + password and MFA
- Password policies comply with current BSI recommendations
 - Use of individual passwords

- Passwords with a minimum length and full complexity. Password length depends on the privileged role, but is at least 10 characters.
- Number of consecutive failed attempts is limited
- Password history
- Key policy in accordance with crypto guidelines
- Encryption of mobile data carriers
 - For Windows: Bitlocker
 - For MAC: Vault
- Autonomous remote maintenance
- Part of the Pa Group's security concept
- Global Secure Access and VPN
- Regular account checks
- Logging of server access at user level
- Encryption during transmission and data at rest
- Physical deletion of data carriers before reuse
- Use of VPN technology
- Use of next-generation firewalls and web application firewalls
- Use of anti-virus software

2.3 Separation control

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

- Defining database rights via PAM
- VLAN concept for a logical separation of network segmentation
- Separation of production, test and inspection environment
- Logical client separation (software side)
- Regular audits (internal/external)

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

3.1 Transfer control

Aspects of the disclosure (transmission) of personal data must be regulated.

- Electronic transmission, data transport, as well as their control.
- Use of encrypted connections (e.g. VPN, HTTPS, SMIME, SFTP, TLS 1.2/1.3)
- Shredder for secure destruction of data
- Data protection boxes for the disposal of confidential paper documents
- Regular audits (at least 1x / y)

3.2 Input control

The traceability and documentation of data management and maintenance must be guaranteed.

- Technical logging of the input, modification and deletion of data at user level for e.g. file shares
- Logging of changes and deletion of data
- Assignment of rights to enter, modify and delete data on the basis of an authorization concept
- Dedicated log server and security operation center (SOC)

4 Availability and Capacity (Art. 32 para. 1 lit. b GDPR)

4.1 Availability control and resilience

The data must be protected against accidental destruction or loss. Systems must have the ability to deal with risk-related changes and have a tolerance and compensatory capacity for disruptions.

- Backup & recovery concept according to the 3-2-1 principle (Immutable Backups)
- Testing Data Recovery
- On-prem systems are designed redundantly across two data centers
- Annual Pen Testing
- Air conditioning in server rooms
- Fire and smoke alarm systems
- Fire extinguishing equipment in server rooms
- Protective power strips in server rooms
- Server rooms equipped with water sensor
- Uninterruptible power supply (UPS)

5 Procedures for Regular Review, Assessment and Evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

5.1 Review procedures

A procedure for regularly reviewing, evaluating and evaluating the effectiveness of the data security measures must be implemented.

- Information Security Baseline (internal security requirement according to ISO27002 and GDPR)
- Company Guidelines (Code of Conduct)
- Notification of new/changed data processing procedures to the data protection officer
- Data protection management in place
- Data protection concept in place
- Regular cross-checking of TOM according to the state of the art according to ISO 27001

6 Technical and Organizational Measures for Mobile Working

The Proalpha Group enables its employees to carry out any work that needs to be done via remote access. To this end, state-of-the-art measures have been taken.

The measures are divided into **technical** measures and **organizational** measures.

6.1 Technical measures

For access to the system from the "home office" or "remote", Proalpha has taken the following measures:

- Access only allowed via business devices
- Endpoints are subject to regular updates
- Applications are made available exclusively via the company portal by IT.
- Access is generally via Global Secure Access. For individual applications, this can also be done via an encrypted VPN connection and MFA
- Windows and MacOS clients are managed via MDM
- Endpoint Security
 - Antivirus Software
 - System encryption
 - System hardening
- Proxy for domain filtering
 - restriction policy
 - untrusted certificates cannot be accepted manually
 - no diagnostic data to Apple
 - User can't manually trust 3rd party apps

6.2 Organizational measures

From an organisational point of view, various supplementary agreements and internal guidelines (in consultation with the works council) have been issued in addition to the measures of the general TOM. This includes, but is not limited to, the following regulations and obligations:

- IT Policy: regulates the secure handling of IT assets (also for private use)
- Commitment to internal guidelines on the use of technical equipment
- Obligation to protect access to work equipment by unauthorised third parties
- Prohibition of the use of own technical equipment (except WLAN, peripheral devices such as keyboard and mouse without driver installation)
- Obligation to keep confidential official documents under lock and key
- Obligation to confidentiality / secrecy
- Obligation to notify change of residence
- Annual training courses