Attachment

Agreement on the processing of personal data on behalf of Art. 28 GDPR / data processing pursuant to Art. 9 DSG

Status: 27/11/2023

The provider provides services for the customer Unified Endpoint Management, which are described in detail in the main contract and defined by ist contract annexes are defined. Insofar as the provider personal data / personal data on behalf of and on behalf of and according to the instructions of the parties conclude the following agreement as an annex to the main contract. The Provider is hereinafter referred to as the Processor / Processor referred to below. The Customer is the Client. Insofar as the provisions of the main contract shall apply.

1. General

(1) The Contractor shall provide the Client with services in the area of Unified Endpoint Management Platform. This includes, among other things, solutions for Mobile Device, Mobile App and Mobile Content Management,Digital Signage Management, Gateway solutions and IoT management. The details are described in the underlying order and in Sec. 3.

(2) The Contractor processes personal data of the Client within the meaning of Art. 4 No. 8 and Art. 28 of Regulation (EU) 2016/679 - General Data Protection Regulation, GDPR for short. This contract regulates the rights and obligations of the parties in connection with the processing of personal data on behalf.

(3) This contract immediately fulfils the requirements of Art. 9 (data processing by processors) of the Swiss Federal Act on Data Protection Act (DSG).

(4) Annex 2 of this agreement also fulfils the legal requirements under Swiss law, namely in accordance with Art. 8 FADP and Art. 3 DPO (Data Protection Ordinance).

(5) Unless otherwise regulated, personal data under the GDPR also means personal data under the FADP.

2. Interpretation, precedence

(1) Where the terms defined in Regulation (EU) 2016/679 are used herein, these terms shall these terms shall have the same meaning as in that Regulation.

(2) In the event of any conflict between these provisions and the provisions of related agreements existing between the parties or subsequently between the parties or subsequently entered into or concluded between the parties, these provisions shall prevail.

3 Subject matter and duration of the contract

(1) Subject matter of the processing

The Contractor processes personal data on behalf data on behalf of the Client. This includes all activities that the Contractor performs in accordance with the service descriptions and the respective contractual agreements with the client and which constitute commissioned processing. The subject matter of the order in detail is from the service agreement in accordance with Annex 1 (description of services) and the underlying order. This also applies if the service descriptions and the respective contractual contractual agreements do not expressly refer to this agreement on commissioned processing.

(2) Duration of the processing

Processing takes place for an unlimited period of time, provided that this is not otherwise agreed in the service descriptions and the respective contractual agreements. Cancellation of the order agreement is possible at the earliest at the end of the service agreement (main contract) with a notice period of 3 (three) months. Cancellation of the main contract shall automatically terminate this order agreement. The possibility of termination without notice for good cause reason remains unaffected by this.

4. Specification of the content of the order

(1) Type and purpose of the intended processing of data: The type of processing includes all types of processing within the meaning of the GDPR. The purpose of the processing of personal data by the Contractor for the Client are specifically described in the service agreement in accordance with Annex 1 (Description of Services).

(2) Types of personal data are all types of types of personal data that the Contractor processes on behalf of the Client. This also includes special

categories of personal data. Object of the processing of personal data are in particular the following data types/categories (list/description of data categories). The detailsare described in Annex 1.

(3) The categories of data subjects affected by the processing are described in Annex 1.

(4) Place of data processing

The provision of the contractually agreed data processing takes place exclusively in Switzerland or a member state of the European Union or in another state party to the Agreement on the European Economic Area. Clause 9 remains unaffected.

5 Obligations of the parties

5.1 Instructions

(1) The Processor shall only process personal data on the documented instructions of the Controller, unless it is obliged to do so under Union law or the law of a Member State to which it is subject, to which it is subject. In such a case, the processor shall inform the controller of these legal requirements prior to the processing, unless the law in question law does not prohibit this on grounds of important public interest. The controller may issue further instructions for the entire duration of the processing of personal data. These instructions must always be documented.

(2) The Client shall confirm verbal instructions without delay (at least in text form).

(3) The Processor shall inform the Controller immediately if it is of the opinion that instructions issued by the Controller are in breach of Regulation (EU) 2016/679 or applicable data protection provisions of the Union or the Member States. The Contractor shall be entitled to suspend the implementation of the corresponding instruction until it is bindingly confirmed or amended by the Client.

(4) If agreed: Only the following named persons (or their representatives if agreed) are authorised to issue instructions to the Client: Described in Appendix 1. Insofar as no expressly named herein, the parties shall agree on this in individual contracts.

5.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) stated in Annex 1, unless it receives further instructions from the controller.

5.3 Security of the processing

(1) The Processor shall take at least the technical and organisational measures listed in Annex 2 to ensure the security of personal data. This includes the protection of the data against a breach of security which, whether accidental or unlawful, results in the destruction, loss, alteration or unauthorised disclosure of or access to the data (hereinafter referred to as "personal data breach"). In assessing the appropriate level of protection, the parties shall take into account the state of the art, the implementation costs the nature, scope, circumstances and purposes of the processing and the risks to the data subjects.

(2) The Processor shall only grant its personnel access to the personal data that are the subject of the processing to the extent necessary for the performance, management and monitoring of the contract. The Processor shall ensure that the persons authorised to process the personal data received have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.

5.4 Commitment to confidentiality and compliance with the requirements of the GDPR, Professional suitability

(1) The Contractor warrants that the persons authorised to process the personal data have undertaken to maintain confidentiality or are subject to an appropriate statutory duty of confidentiality. The Contractor warrants that the persons authorised to process the personal data compliance with the requirements of the GDPR have been obligated. The client has the right to upon request by inspecting the declarations of commitment/the content and scope of the obligation by inspecting the of the obligation.

(2) The Contractor shall only use professionally qualifiedpersons for the processing of personal data. It shall ensure regular training and instruction in matters of data protection and data protection and information security.

5.5 Documentation and compliance with the provisions

(1) The parties must be able to demonstrate compliance with the provisions.

(2) The Processor shall process requests from the Controller regarding the processing of data in accordance with these provisions promptly and in an appropriate manner.

(3) The Processor shall provide the Controller with all information necessary to demonstrate

compliance with the obligations laid down in these provisions and arising directly from Regulation (EU) 2016/679. At the request of the controller processor shall also allow the processing activities covered by these provisions to be audited at appropriate intervals or if there are indications of non-compliance and contributes to such an audit. When deciding on an inspection or audit, the controller may take into account relevant certifications of the processor may be taken into account.

(4) The controller may carry out the audit itself or commission an independent auditor. The audits may also include inspections of the premises or physical facilities of the processor and, where appropriate, shall be carried out with reasonable prior notice.

(5) The parties shall make the information referred to in this clause, including the results of audits, available to the competent supervisory authority or authorities upon request

(6) The Client and the Contractor shall cooperate with the supervisory authority in the fulfilment of its tasks upon request. This shall also apply insofar as a competent authority within the framework of administrative offence or criminal proceedings in relation to the processing of personal data during the processing at the Contractor.

(7) Insofar as the client is subject to an inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support the Client to the best of ist best endeavours.

6. International data transfers

(1) Any transfer of data by the processor to a third country or an international organisation shall take place exclusively on the basis of documented instructions from the basis of documented instructions from the controller or to comply with a specific provision under Union or Member State law to which the processor is subject and shall comply with Chapter V of Regulation (EU) 2016/679.

(2) The controller agrees that in cases where the processor or a sub-processor for the performance of certain processing activities (on behalf of the controller) and these processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor may ensure compliance by using standard contractual clauses adopted by the Commission pursuant to Article 46(2) of Regulation (EU)2016/679, provided that the conditions for the application of these standard contractual clauses are met. Art. 44 et seq. GDPR otherwise remains unaffected.

7. Technical and organisational measures (TOM) / data security pursuant to Art. 8 GDPR

(1) The Contractor shall ensure the implementation and necessary technical and organisational measures set out in the run-up to the award of the contract before the start of processing, in particular with regard to the specific execution of the order and submit it to the client for review. If accepted by the client, the documented measures shall form the basis of the order. Insofar as the review of the audit reveals a need for adjustment, this implemented by mutual agreement.

(2) The Contractor shall provide security in accordance with Art. 28 para. 3 lit. c), 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are data security measures and to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art technology, the implementation costs and the type, the scope and purposes of the processing and the different probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR have to be considered. The details are set out in Annex 2.

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative adequate measures. In doing so, the security level of the measures may not be undercut. Significant changes must be documented.

8. Rectification, restriction and erasure of data

The Contractor may not process the data on its own authority, but only after documented instructions from the client. If a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay.

9. Quality assurance and other obligations of the Contractor

In addition to complying with legal obligations pursuant to Art. 28 to 33 GDPR, the Contractor shall in particular ensure compliance with the following requirements:

(1) The Contractor is obliged to maintain confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b), 29, 32 para. 4 GDPR. The contractor shall only use employees to carry out the work, who are obliged to maintain confidentiality and who have been confidentiality and have previously been familiarised with the data protection provisions relevant to them. The contractor and any person subordinate to the Contractor who has access to personal data may only process this data in accordance with the instructions of the Client, including the authorisations granted in this contract unless they are legally obliged to process the data.

(2) The implementation of and compliance with all technical and organisational measures required for this contract pursuant to Art. 28 para. 3 sentence 2 lit. c), 32 GDPR is regulated in Annex 2.

(3) The Contractor shall regularly monitor the internal processes and the technical and organisational measures in order to ensure that the processing in his area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject are guaranteed.

10. Use of subcontracted processors

(1) The Client shall grant the Contractor the authorisation in principle to use sub-processors. At the time of contract is signed, the following sub-processors exist (list):

- Host Europe GmbH, Hansestrasse 111, 51149 Cologne

- AppTec Services GmbH, Engelbergerstr. 21, D79106 Freiburg, Germany

(2) Outsourcing to other sub-processors or changing existing sub-processors is permitted. The processor shall inform the controller at least 4 weeks in advance of any intended changes to this list by adding or replacing sub-processors and of sub-processors and shall thus give the controller sufficient time to take appropriate measures before processor(s) concerned to object to these changes. The processor shall provide the controller with the necessary information to enable the controller to exercise its right to object.

(3) If the processor engages a sub-processor to carry out certain processing activities (on behalf of the controller), this engagement must be made by way of a contract that essentially imposes the same data protection obligations on the sub-processor as those that apply to the processor in accordance with these provisions.

(4) The processor shall be fully liable to the fully liable to the controller for ensuring that the Processor fulfils its obligations under the contract concluded with the processor contract concluded with the processor.

(5) If the sub-processor provides the agreed service outside the EU/EEA, the processor shall ensure the EEA, the Contractor shall ensure the admissibility under data protection law through appropriate measures and guarantees in accordance with Art. 44 et seq. GDPR.

(6) If the Contractor places orders with other processors, the Contractor shall be responsible for transferring its data protection obligations under this contract to the other processor.

11. Support obligations of the contractor

(1) The processor shall inform the controller without undue delay of any request that it received from the data subject. It shall not respond to the request itself unless it has been authorised to do so by the controller.

(2) Taking into account the nature of the processing processor shall assist the controller in the fulfilment of the controller's obligation to respond to requests from data subjects to exercise their rights answer

(3) The Processor shall support the Controller in complying with the obligations set out in the GDPRobligations for the security of personal data, safeguarding the rights of data subjects, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes among others

a) ensuring an appropriate level of protection through technical and organisational measures that organisational measures that take into account the circumstances and processing as well as the predicted probability and severity of a possible breach due to security vulnerabilities.

b) the obligation to report personal data breaches to the client without undue delay (cf. to the Client without undue delay (see Section 13).

c) the obligation to support the Client in its duty to inform the data subject and in this context to make all relevant information immediately in this context.

d) the support of the controller in complying with the compliance with the obligations set out in

Articles 32 to 36 GDPR taking into account the nature of the processing and the information available to it.

e) the support of the client for its data protection impact assessment.

12. Notification of a personal data breach

12.1 Breach of the protection of data processed by the controller

In the event of a personal data breach in connection with the data processed by the controller, the processor shall assist the controller as follows:

a) promptly notify the personal data breach to the competent supervisory authority or authorities without undue delay after the controller becomes aware of the personal data breach, where relevant (unless the personal data breach does not give rise to a risk to the personal rights and freedoms of natural persons);

(b) when obtaining the following information, required by Article 33(3) of Regulation (EU) 2016/679] in the controller's notification, which shall include at least the following information:

1) the nature of the personal data, where possible, with an indication of the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2) the likely consequences of the personal data breach

3) the measures taken or proposed to be taken by the controller to address the personal data breach; and where appropriate, measures to mitigate its possible adverse effects.

If and to the extent that not all of this information can be provided at the same time, the original notification will contain the information available at that time and further information shall be provided subsequently without undue delay as soon as it becomes available;

(c) when complying with the obligation under Article 34 of Regulation (EU) 2016/679, the data subject of the personal data breach, without undue delay is likely to result in a high risk to the rights and freedoms of natural persons

12.2 Breach of the protection of data processed by the processor

In the event of a personal data breach in connection with the data processed by the Processor, the Processor shall notify the Controller without undue delay after becoming aware of the breach. This notification must contain at least the following information

(a) a description of the nature of the breach (where possible, specifying the categories and approximate number of data subjects concerned and the approximate number of data records concerned);

b) contact details of a contact point where furthe information about the personal data breach can be obtained;

(c) the likely consequences and the measures taken or proposed to address of the personal data breach, including mitigating measures to mitigate ist possible adverse effects.

If and to the extent that not all of this information can be provided at the same time, the initial notification will contain the information available at that time and further information will be provided as soon as it becomes available without undue delay thereafter.

13. Erasure and return of personal data

(1) Copies or duplicates of the data will not be made without the knowledge of the client. The only exceptions to this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data that is required in order to comply with statutory retention obligations.

(2) After completion of the provision of the processing services, the Contractor either deletes all personal data or returns it to the customer, unless it is required by law there is an obligation to store the personal data or if this is evident from the service descriptions and the respective contractual agreements.

(3) Documentation that serves as proof of the orderly and proper data processing shall be retained by the Contractor beyond the end of the contract in accordance with the respective end of the contract. The Contractor may hand them over to the Client at the end of the contract.

(4) The Contractor waives the assertion of rights of retention within the meaning of § 273 BGB on the personal data processed by him.

14. Severability clause

Should individual provisions of this agreement prove to be invalid, validity of the remaining provisions shall not be affected.

The invalid provision shall be replaced by a provision that the parties would have agreed upon if they had considered the invalidity of the respective point when concluding the contract. Insofar as agreement contains an unintentional loophole, this shall be replaced by a provision that the parties would have the need to regulate the respective point when concluding the contract.

15. Formal requirement

Amendments and additions to these terms and conditions and all their components - including any assurances of the Contractor - must be made in GDPR in writing, which may also be in an electronic format, and the express reference to the fact that it is an amendment or supplement to these terms and conditions. This also applies to the waiver of this formal requirement.

16. Final provisions

(1) The law of the main contract shall apply to this order processing and all processing activities performed in this context.

(2) The place of jurisdiction for all disputes arising from or in connection with this agreement, regardless of the legal grounds is agreed in the main contract.

(3) Amendments to this agreement must be madewritten form. This also applies to the cancellation of the written form requirement.

(4) Should provisions of this agreement be or become invalid, this shall not affect the validity of the remaining provisions. In this case invalid provision shall be replaced by the statutory provision(s).

The following annexes form an integral part of this agreement

Annex 1 - Description of the services, type of data, categories of data subjects, authorised persons of the client

Annex 2 - Technical and organisational measures / data security

Annex 1 - Description of the services, duration of processing, type of data, categories of data subjects, persons authorised to issue instructions to the client

1. Description of the services (type of processing and purposes)

The Contractor provides services for the Client in the area of Unified Endpoint Management Platform. This includes solutions for mobile device, mobile app and mobile content management, digital signage management, gateway solutions and IoT management. The object of the commissioned data processing is the provision (hosting) of the AppTec Software & AddOns for use by the client by means of access via the Internet. The details are described in the underlying order.

2. Duration of the processing: see section 3 of the DP

3. Type of personal data (please tick as appropriate)

☒ **Personal master data**

☒ **Communication data**

☒ **Login data**

☒ **Device data assigned to persons**

☒ **Log files and log data**

☒ **IP addresses, geolocalisation data**

☒ **Browsing history, favourites**

☒ **Email communication and attachments**

☒ **Usage data, unless recorded above**

☐ **Other (please describe)**

4. Categories of data subjects (please tick as appropriate)

☒ **Employees of the client**

☒ **Customers, business partners and service providers**

☒ **(Business) contacts of the client**

☒ **Enquirers / interested parties of the client**

☒ **Email (sender and recipient)**

☒ **Telephony (callers and called parties)**

☒ **All other persons who are processed on the client's systems and whose personal data is processed by the contractor as part of the provision of services**

Annex 2 - Technical and organisational measures pursuant to Art. 32 GDPR / Data security pursuant to Art. 9 FADP / Art. 3 DPA

A. Pseudonymisation Encryption (Art. 32 para. 1 lit. a) GDPR)

Measures taken:

- ☒ Kunden- und Lieferantenaudits
- ☒ Use of VPN
- ☒ Transport encryption for remote maintenance access
- ☒ Encryption of mobile devices (smart phone, tablet)
- ☒ Hard drive encryption laptop

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

1. Access control

Ensuring that only authorised persons have access to the business premises

Measures taken:

- ☒ Business premises of the client can only be entered through main entrances and are protected by electronic access control systems, key systems, the use of alarm systems and special structural measures.
- ☒ Visitor registration, escorting of visitors
- ☒ Only the relevant employees have access to the offices
- ☒ Keys / key allocation: Organisational instructions exist for issuing keys. The site manager is responsible for managing the keys.
- ☒ Door security (electric door openers, etc.)
- ☒ Video surveillance

2. Access control system

Ensuring that only employees of the responsible body or workers who are obliged to do so within the scope of commissioned processing are authorised to enter the designated area of responsibility and process the corresponding data with user identification:

Measures taken:

- ☒ A password and user administration system is in place. User accounts are personalised.
- ☒ A change cycle for user passwords specified by the system is set up at all computer workstations (change cycle)
- ☒ Maintenance work requires our express consent. They may only be started if the maintenance personnel have logged in with user ID and password.
- ☒ Accesses for authentication on the system are generated exclusively new and personalised
- ☒ Digital certificates

3. Accessing control

Ensuring that those authorised to use an automated processing system only have access to the personal data covered by their access authorisation:

Measures taken:

- ⌦ Screen lock
- ⌦ Authentication with user and password
- ⌦ Contractors are only granted the access rights they actually need to carry out maintenance work
- ⌦ A range of hardware and software identification measures, encryption of data during data transfer and a multi-level access and usage control procedure prevent unauthorised access to the stored data and unauthorised knowledge of it
- ⌦ User-related logging of (incorrect) logins
- ⌦ It is ensured that IT personnel can only access stored personal data to the extent that this is necessary for personal data to the extent that this is absolutely necessary to carry out maintenance work
- ⌦ An authorisation concept ensures that personal data and other data worthy of protection are protected against accidental destruction or loss
- ⌦ Use of document destruction
- ⌦ Proper destruction and/or deletion of data storage media (DIN 66398)

4. User control

Ensuring that unauthorised persons are prevented from using automated processing systems with the aid of data transmission equipment:

Measures taken:

- ⌦ Use of authorisation concept
- ⌦ Group authorisations are flat and clearly structured and are not used in cascade
- ⌦ Defined authorisation profiles for the various functional areas are explicitly assigned and administered centrally

5. Memory control

Prevention of unauthorised input of personal data and unauthorised access, modification and deletion of stored personal data.

The plausibility check of the data entry takes place on audit-relevant fields and is validated according to the associated processes.

Measures taken:

- ⌦ Logging of system utilisation and evaluation of the logging
- ⌦ A multi-stage logging process ensures that no data changes can be made unnoticed

6. Separability

Ensuring that personal data collected for different purposes is processed separately are processed separately:

The principle of functional separation applies in all key areas; this means that all departments involved in data processing are functionally and organisationally separate. Data worthy of protection is only made available to employees to the extent that it is absolutely necessary for the assigned lawful fulfilment of tasks.

Measures taken:

- ⌦ Separation takes place via the access regulations
- ⌦ Data worthy of protection is only made available to employees to the extent that it is absolutely necessary for the assigned is absolutely necessary for the assigned lawful fulfilment of tasks
- ⌦ The principle of segregation of duties applies in all important areas
- ⌦ Separation of productive and test systems as well as folder structures and databases

C. Integrity (Art. 32 para. 1 lit. c) GDPR)

7. Data integrity

Ensuring that stored personal data cannot be damaged by system malfunctions:

Measures taken:

⌦ Software-based exclusion (client separation, file separation)

⌦ Use of centralised patch management for software components

8. Transport control

Ensure that the confidentiality and integrity of personal data is protected during the transmission of personal data and the transport of data carriers.

Measures taken:

⌦ Data is only transmitted in encrypted form (transport encryption for remote maintenance access)

⌦ Guidelines and procedural instructions exist in which the use and correct handling of mobile and correct handling of mobile data carriers, devices and means of communication. There is also a guideline for dealing with faulty print products.

⌦ Strict guidelines and work instructions at the contractor ensure that unauthorised disclosure or removal of data is prevented

⌦ Disposal material with content worthy of protection is destroyed in compliance with the security levels of the degree of destruction according to DIN 66399

9. Transfer control

Ensuring that it is possible to check and establish to which bodies personal data has been or can be transmitted or made available with the aid of data transmission equipment.

Measures taken:

⌦ Logging of the data transfer point/routes, which can be analysed in the event of suspicion

⌦ Technical protection is provided by firewalls and proxy systems

⌦ Where technically possible and economically viable, suitable encryption technologies are used (see transport encryption for remote maintenance)

10. Input control

Ensuring that it is subsequently possible to verify and establish which personal data entered or modified in automated processing systems, at what time and by whom:

All personal data collected will only be processed in accordance with the applicable regulations on the protection of personal data, only for the purpose of the respective order processing and for the protection of our own legitimate business interests with regard to advising and supporting customers and for the fulfilment of employment contracts.

Measures taken:

⌦ Logging of system usage and evaluation of the logging

⌦ A multi-stage logging procedure ensures that no data changes can be made unnoticed

⌦ Implementation of training measures for the use of software

- ⌦ All employees receive data protection training at regular intervals
- ⌦ Random checks of data processing

11. Reliability

Ensuring that all system functions are available and that any malfunctions are reported:

Measures taken:

- ⌦ Event logging of the systems with reporting of malfunctions
- ⌦ Maintenance contracts and SLA agreements

12. order control

Ensuring that personal data processed on behalf of the client can only be processed in accordance with the client's instructions:

Measures taken:

- ⌦ All service providers who have the opportunity to view personal data will be informed in accordance with the Federal Data Protection Act on data secrecy and purpose limitation in the case of commissioned processing.
- ⌦ The data submitted for processing is only processed in accordance with the statutory provisions within the framework of the instructions and, in particular, is not passed on to unauthorised third parties; exceptions to the specific framework of instructions only apply to processing for technical reasons, e.g. for internal security purposes.
- ⌦ The framework of instructions is defined in particular by the written contract for data processing on behalf of in the order, taking into account the mandatory content, as well as the application description of the service.
- ⌦ Agreements with processors in accordance with Art. 28 GDPR.
- ⌦ Intercompany agreements in accordance with Art. 28 GDPR with affiliated companies that process data on behalf of others.
- ⌦ Standard contractual clauses (SCC) for the transfer of data to third countries. Alternatively, for data transfers to the USA (Data Privacy Framework - DPF).
- ⌦ Order-related information is provided exclusively to the client or in accordance with their instructions.
- ⌦ Comprehensive contractually guaranteed control rights of the client.

D. Availability and resilience (Art. 32 para. 1 lit. c) GDPR)

13. Availability Control

Guarantee that personal data is protected against destruction or loss:

A multi-level protocol procedure ensures, as far as possible, that no data changes are unnoticed can be made. It is logged on both the client and the server side. The focus of the logging is on application, system and security levels.

Measures taken:

- ⌦ There are guidelines and procedures for the secure operation of the IT environment. Also Anti-virus,

  backup, and archiving measures exist.

14. Recoverability

Ensure that systems used can be restored in the event of a malfunction:

Numerous data protection measures ensure that personal and other data is protected against accidental destruction or loss.

Measures taken:

- ⌦ There are emergency and recovery plans. Backups are performed daily and weekly according to a defined backup plan.
- ⌦ Use of raid systems and mirroring of data stocks
- ⌦ Multiple automated and unauthorized outsourcing of backups

15. Disk Control

Prevention of unauthorized reading, copying, modification or deletion of media:

Measures taken:

- ⌦ Security precautions ensure that unauthorized removal of media from security areas is prevented
- ⌦ Inventory of all disks

E. Procedure for regular review, evaluation and evaluation (Art. 32 para. 1 lit. d) GDPR)

Measures taken:

- ⌦ Regular test of the applications
- ⌦ Review of measures in the context of the effectiveness control of the information security management system (ISMS - in accordance with DIN ISO/IEC 27001)
- ⌦ Continuous improvement process within the framework of ISMS
- ⌦ Appointment of a Data Protection Officer
- ⌦ The data protection officer can be reached as follows: datenschutzbeauftragter@apptec360.com
- ⌦ Regular data protection/and IT security training of authorized employees
- ⌦ Periodic verification of processing directories and technical and organisational measures and if necessary
- ⌦ Audits of auditors
- ⌦ Customer and supplier audits

Hint: Translated version. The original version was written in German.