Information Type: Restricted

Version: 2022-07

Data Processing Agreement (DPA)

According to Article 28 (3) GDPR
for Managed Services (Managed Cloud and Application Management)

between:

Client (according to Service Level Agreement / “Leistungsvereinbarung”)

and:

NTT DATA Business Solutions Global Managed Services GmbH
Philipp-Reis-Strasse 2
02625 Bautzen

(hereinafter referred to as "**Contractor** ")

§ 1 Preamble and Scope of Application

The Contractor processes Personal Data in the course of its services for the Client in accordance with Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council (the General Data Protection Regulation - "GDPR").

The terms used in this contract are applied in accordance with their definition in the GDPR. Unless expressly provided otherwise in this contract or in the applicable statutory provisions, electronic form (e.g. e-mail) shall also suffice for the submission of a written declaration.

§ 2 Subject Matter and Duration of the Contract

(1) This Data Processing Agreement (hereinafter referred to as the "Agreement") shall apply to all data processing activities performed by the Contractor for the Client within the scope of the service(s) listed in the Annex / Annexes.

(2) Changes to the object of processing and changes to the process shall be agreed jointly between the Client and the Contractor and shall be set out in writing or in a documented electronic format.

(3) This contract is valid for an indefinite period of time and remains in force until the last service contract has expired or the either party terminates it by providing the other with 30 days' notice in writing. This Agreement may be terminated immediately by either party if the other has materially breached the terms of the Agreement and such breach is not remedied within 15 days.

§ 3 Details of the Data Processing

(1) The nature and purpose of the processing of Personal Data carried out by the Contractor on behalf of the Client are described in the respective Service Agreement(s) and, in particular, in Annex 1 to this Contract. The Contractor is entitled to fulfil the subject of the Service Agreement in accordance with the provisions of this Agreement to carry out all necessary processing steps.

(2) The types of data concerned and the categories of data subjects by the processing are described in Annex 1 to this contract.

§ 4 Obligation of the Contractor

(1) The Contractor shall process Personal Data only to the extent necessary for the performance of the Service Agreement(s), in accordance with this Agreement and applicable law.

(2) The Contractor shall refrain from any use and processing for private, personal or other commercial or business purposes. The Contractor shall avoid access to the Client's data as far as possible. If data access is necessary, the client is obliged to limit it to the minimum possible for the specific fulfilment of the order.

(3) The contractor is obliged to exercise the necessary care to ensure that all persons entrusted with the data processing comply with the statutory data protection provisions, process data exclusively in accordance with the client's instructions and do not pass on the data obtained from the client to third

parties or use it in any other deviating manner. The Contractor ensures that all persons entrusted with the processing have been bound to data secrecy.

(4) The Contractor shall take all measures required under Article 32 GDPR. Further details are regulated in § 8 of this contract (Technical and organizational measures) as well as Annex 2.

(5) The Contractor shall inform the Client without delay if the Contractor becomes aware of any breaches of the protection of the Personal Data processed for the Client (e.g. unauthorized access). The Contractor shall support the Client in complying with the reporting obligations in accordance with applicable law.

(6) The contact details of the Contractor's Data Protection Officer are datenschutz-solutions-de@nttdata.com.

(7) In the event of serious disruptions to the operational process which create risks for the Client's Personal Data, in the event of justified suspicion of data protection violations or in the event of other irregularities in the processing of the Client's data, the Contractor shall inform the Client without undue delay. The same shall apply if the Contractor is of the opinion that the security measures agreed between the parties do no longer comply with the applicable legal requirements. The Contractor is aware that the Client is obliged to comprehensively document all breaches of the protection of Personal Data and, if necessary, to report them without undue delay to the supervisory authorities and the persons affected. The Contractor shall also inform the Client of the supervisory authority's control actions and measures insofar as they relate to this contract. This shall also apply if a competent authority investigates the data processing at the Contractor as part of administrative offence or criminal proceedings.

In such a case, the parties may agree on an interruption of the processing activity. The Contractor shall inform the Client of any such interruption of the processing activity. The Contractor shall notify the Client of the subsequent outcome of any inspection by the supervisory authorities or other competent authorities with regard to this Agreement. The Contractor shall rectify the identified deficiencies without undue delay and shall take appropriate measures to remedy such deficiencies.

(8) If Personal Data or Personal Data storage devices of the Client are endangered by seizure, confiscation, insolvency or composition proceedings or other events or measures by third parties, the Contractor shall immediately inform the Client of these circumstances.

(9) The Contractor shall support the Client within the scope of its possibilities in fulfilling the requests of data subjects pursuant to chapter III of the GDPR and in complying with the obligations set out in articles 33 to 36 of the GDPR.

§ 5 Responsibilities of the Client

(1) The Client is responsible for compliance with the statutory provisions of data protection law, in particular for the lawfulness of the data transfer to the Contractor and the data processing. In addition, the Client, being the Controller of the Personal Data, is solely responsible for safeguarding the rights of the data subjects pursuant to articles 12 to 22 of the GDPR ("Controller" within the meaning of Article 4 No. 7 of the GDPR).

(2) The Client shall inform the Contractor immediately and in full about any errors or irregularities in the processing results or data protection provisions or, for whatever reason, if he is no longer entitled to pass on the Personal Data to the Contractor. Furthermore, this duty to inform exists if he is exposed to control actions and measures of the competent supervisory or specialist authorities in the context of an administrative offence, criminal proceedings or liability claims of a data subject or a third party, insofar as these circumstances relate to or may affect this contract. With regard to an interruption of data processing, the regulations of § 4 (8) of this contract apply.

(3) If a claim is made against the Client by a data subject with regard to one of the rights defined in Article 82 of the GDPR, the Client shall be independently responsible for defending this claim. The Contractor may support the Client in this matter by means of a special Agreement.

(4) The Client shall inform the Contractor of the details of the data protection officer(s) or contact person(s) for data protection and for all data protection issues arising from this Agreement as well as the respective persons authorized to issue instructions. In the event of a change or prolonged prevention of the contact person(s), details of the successors or authorized representatives shall be communicated to the contractual partner without delay.

(5) The client is obliged to treat all knowledge of the contractor's business secrets and data security measures obtained within the framework of the contractual relationship as confidential. This obligation shall remain in force even after termination of this contract.

§ 6 Instruction Rights of the Client

(1) The Contractor shall process the data made available to it in accordance with the provisions in § 4 of this contract only in accordance with documented instructions from the Client and within the framework of the Agreements made. The Client has the right and the obligation to issue instructions on the type, scope and procedure of the processing activities in relation to the service(s) provided by the Contractor.

(2) The instructions are initially determined by this contract and the corresponding service contract(s) in accordance with § 2 (1) of this contract. They may be subsequently amended, supplemented and / or replaced by the Client by individual instructions or in an agreed electronic format (e.g. ticket system, fax or e-mail) to the Contractor. Instructions or orders not provided for in the contract shall be treated as a request for a change in performance of the service(s), for which a corresponding change Agreement in written form is required. Verbal instructions shall be confirmed immediately in writing or in documented electronic form; the Contractor shall be entitled to suspend the execution of an instruction until it has been confirmed.

(3) The Contractor shall inform the Client without delay if it is of the opinion that an instruction violates provisions of data protection law. The Contractor shall be entitled to suspend the execution of the relevant instruction until its legality is confirmed by the Client or it becomes a legally permissible instruction.

§ 7 Data Processing Outside of the EU/EEA

(1) Where relevant in individual cases, processing may be carried out by the contractor in a third country outside the EU/EEA.

(2) The provision of contractually agreed data processing outside the EU/EEA or Switzerland, in particular the transfer of data to or from a third country as well as the transfer of Personal Data, requires compliance with the following requirements in accordance with article 44 et seq. GDPR:

- if the recipient, the country or territory where Personal Data are processed or accessed, ensures an adequate level of protection for the rights and freedoms of data subjects with regard to the processing of Personal Data, as determined by the European Commission; or
- if standard contractual clauses (SCCs based on Schrems II) have been agreed with the respective recipients or countries.

(3) The EU Standard Contractual Clauses (2021 version based on Schrems II decision by the European Court of Justice) must be applied by the Contractor where an international transfer takes place to a country which does not ensure an adequate level of protection for the rights and freedoms of data subjects with regard to the processing of Personal Data, as determined by the European Commission.

(4) In case of sub-processors from third countries, the Contractor must ensure that they provide an adequate level of protection for the transferred Personal Data. The Contractor must require its sub-processors to conclude data processing contracts and/or standard contractual clauses prior to the processing of Personal Data by the sub-processor, as soon as this is necessary. These contracts must resemble the data processing Agreement(s) between the Contractor and Client and ensure a similar level of data protection. The Contractor enforces the standard contractual clauses (2021 version based on Schrems II decision by the European Court of Justice) against the sub-processor on behalf of the Data Controller where a direct enforcement right under data protection law is not available, which the Contractor is hereby expressly authorized to do by the Client.

§ 8 Technical and organizational Measures

(1) The Contractor shall organize the internal organization within its area of responsibility in such a way that the specific requirements of the relevant data protection provisions are complied with and appropriate technical and organizational measures are taken to ensure a level of protection appropriate to the risk to the rights and freedoms of the data subjects which corresponds to the current state of the art for the respective processing activities and meets the requirements of Article 32 of the GDPR.

(2) The Client shall inspect the Contractor's documented technical and organizational measures (Appendix 2) as part of a preliminary review before the data processing by the Contractor begins. Any necessary adjustments to these measures, taking into account the risk associated with the specific processing activity, shall be communicated by the Client to the Contractor and decided by mutual Agreement between the parties by adjusting the provided Technical and Organizational Measures (Appendix 2).

(3) The agreed measures are documented in Annex 2 to this contract. The Client is aware of these technical and organizational measures and is responsible for ensuring that they provide a level of security appropriate to the risks to the rights and freedoms of the data to be processed by the Contractor.

(4) The Contractor reserves the right to adapt the technical and organizational measures from time to time, but must ensure that the level of protection provided for the processing does not fall below the appropriate minimum level of security to comply with article 35 GDPR. The Contractor shall inform the Client of any material changes to the Technical and Organizational Measures (Appendix 2).

(5) The Contractor shall regularly monitor its internal processes and technical and organizational measures to ensure that the processing of the Client's Personal Data is carried out in accordance with the requirements of applicable data protection law (in particular, article 32 of the GDPR). The Contractor shall provide the Client with evidence by appropriate means that it complies with the obligations and measures set out in this Contract, if reasonably requested by the Client.

§ 9 Rights of Data Subjects

(1) The rights of the data subjects arising from the collection, processing and use of their data by the contractor must always be asserted against the client. The Client is responsible for safeguarding these rights. In particular, the Client shall be responsible for notifying the data subjects, providing information, correcting, deleting and blocking Personal Data. The Client shall inform the Contractor without delay of the necessary activities to realize such rights of data subjects.

(2) If a data subject contacts the Contractor directly, the Contractor shall immediately forward this request to the Client and refer the data subject to the Client, provided that it is possible to connect the request to the Client on the basis of the information provided by the data subject.

(3) The Contractor shall support the Client in responding to and fulfilling requests by data subjects. For example, if the Client is obliged under applicable data protection law to provide a data subject with information about the collection, processing or use of his Personal Data, the Contractor shall, upon request, provide the Client with the information required for this to the extent possible.

(4) The Contractor shall not correct, delete or restrict the Personal Data processed on behalf of the Client; such action by the Contractor is only permissible following documented instructions from the Client.

§ 10 Audit Rights of the Client

(1) The Client shall be entitled to control by appropriate means the Contractor's technical and organizational measures before the start of the processing and thereafter by obtaining information provided by the Contractor, requesting specific reasonable evidence from the Contractor or by means of self-assessments by the Contractor. For example, the evidence can be provided by the following types of information:

- Conduct of a self-audit (current attestations, reports or report extracts from independent bodies (e.g. auditors, data protection officers, auditors, IT security department, data protection auditors, quality auditors).

- Internal company rules of conduct / processes, including evidence of compliance with the such.
- Certificate for information security (e.g. ISO 27001).
- A suitable certification according to an IT security or data protection audit (e.g. according to BSI-Grundschutz).

(2) The Client and the Contractor can agree that evidence can also be provided by other documents / certificates.

(3) If the control measures according to § 10 (1) of this contract do not result in clarity for the Client, an audit by the Client or an auditor commissioned by the Client will be agreed upon by the parties.

(4) If, in individual cases, controls by the Client or an external auditor acting on behalf of the Client are required, these may be carried out by the Client's Data Protection Officer and other parties appointed by the Client after informing the Contractor's Data Protection Officer in good time, that the measures for compliance with the technical and organizational requirements of the relevant data protection laws are suitable for processing by the Contractor. The audit takes place on the Contractor's premises during normal business hours without disrupting operations. The Contractor may make audits dependent on the prior signing of a confidentiality Agreement regarding the individual audit, e.g. in regards of the data of other customers and the technical and organizational measures put in place.

(5) If the Client commissions a third party to carry out the inspection, the Client shall also oblige the third party in writing to maintain secrecy and confidentiality, unless the third party is subject to a professional duty of confidentiality. If the Client's auditor is in a competitive relationship with the Contractor, the Contractor has the right to request another auditor.

§ 11 Subcontractors

(1) Subcontracting business relationships within the meaning of this provision shall be understood to mean services which are provided by subcontractors (further data processors) and which relate directly to the performance of the service(s) under this Data Processing Agreement and its connected service contract(s). Not defined as subcontracting business relationships are additional ancillary services used by the Contractor, e.g. in the form of telecommunications services, postal/transport services, maintenance and user services and/or the disposal of data carriers or documents as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Contractor is obliged to conclude appropriate and legally compliant contractual regulations and control measures to ensure the protection and security of the Client's data, even in case of such outsourced ancillary services.

(2) The Contractor may engage subcontractors such as affiliated companies or external service providers to process Personal Data of the Client. If the Client has justified concerns in regards of a chosen subcontractor, Client may veto the chosen subcontractor.

(3) The Contractor must conclude contracts with subcontractors involved in the data processing. These contracts shall impose confidentiality, data protection and data security obligations on the subcontractor similar to the level of data protection and security offered by this contract. The

Contractor shall on a regular basis (taking into consideration the risk based approach of the GDPR) review and verify the subcontractor's compliance with these obligations. The Client is at all times entitled to receive from the Contractor, upon written request, an overview of the subcontractors used for the service as well as information on the content of the contractual agreements, the implementation of the data protection obligations of the subcontractor as well as verification of the subcontractor controls by the Contractor.

(4) Any data transfer and data processing by a subcontractor of the Contractor shall not commence before the subcontractor complies with all requirements similar to this Agreement.

(5) If the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall take all necessary measures to ensure that the processing is in compliance with the EU's GDPR requirements, in particular article 46 (2) c) (Standard Contractual Clauses). Section 7 of this contract shall apply accordingly.

§ 12 Deletion and Return of Personal Data

(1) After termination of the service contract or at any other time, the Contractor shall delete, destroy or return to the Client, at the Client's discretion, the Personal Data provided by the Client, the Personal Data collected, processed and/or used for the Client, the processing and usage results created by the Client as well as any copies thereof and the documents received from the Client in connection with the contractual relationship. If the disclosure or return of the data or any copies thereof is not possible for technical reasons (e.g. due to electronic storage on permanently installed or - insofar as permissible under data protection law - jointly used media) or if deletion/destruction is requested by the Client, the corresponding data shall be deleted by the Contractor in consultation with the Client and in compliance with data protection laws.

(2) At the request of the Client, electronically stored data shall either be provided in commercially available format on electronic data carriers or transferred online. This shall not apply to backup copies, insofar as these are required to ensure proper data processing, and to data required to fulfil statutory retention obligations. The Contractor may make these accessible to the Client at the end of the contract in order to discharge the Contractor.

(3) The Contractor shall confirm the deletion/destruction to the Client in writing or by e-mail. Further legal deletion obligations and deletion claims remain unaffected by the above regulations.

§ 13 Final Provision

(1) The annexes listed below are an integral part of this contract. Amendments or supplements to this contract or any of its components must be made in writing, unless expressly agreed otherwise. This also applies to a waiver of this formal requirement. No additional side Agreements have been concluded by the parties.

(2) The contract, amendments to the contract and future side Agreements must be concluded in writing; this may also be done electronically. Notices/information, declarations of consent, declarations of approval and confirmations may be sent by e-mail.

Should individual provisions of this contract be invalid or unenforceable in whole or in part or become invalid or unenforceable due to a change in the legal situation occurring after conclusion of the contract, this shall not affect the validity of the remaining provisions of the contract as a whole. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision which comes as close as possible to the purpose pursued by the invalid provision. The parties shall make a corresponding provision that meets this objective.

List of assets

Appendix 1: Data processing activities, nature and purpose, types of data and data subjects

Appendix 2: Technical and organizational measures

Appendix 1: Managed Services

(1) Service description

Preamble: Managed Services

It's an umbrella for Application Management Services (AMS), Managed Cloud Services (MCS), Maintenance and parts of our subscription business. The related services, provided to our customers, are described in detail in the global Managed Services Portfolio of NTT Data Business Solutions. NTTD Business Solutions ticket system based on SAP Solution Manager provides an up-to-date knowledge base containing entire history of customer's tickets and comprehensive information about problem and resolution contents.

Service description: Managed Cloud Services (MCS)

General term for SAP basis and infrastructure services in own Data Centers, on hyperscaler infrastructure or as remote service. It consists of full management of cloud infrastructure and technical operations of applications, which run on top of these infrastructures as well as long-term technical support and operations of applications.

The service includes in detail:

- Complete hosting of SAP application system landscapes, including development, quality assurance and production systems
- Provisioning of all application layers, i.e. database, SAP application servers and additional system components like gateway systems, Adobe Document Services and Fiori Frontend systems
- Complete technical monitoring and management of SAP Basis components
- High availability SLA, including disaster recovery options, to meet the high expectations on application availability for company critical applications
- Close integration into customer SAP backend systems for seamless exchange of data with SAP S/4HANA, ERP, CRM and SCM
- Service applies to virtually all available SAP software products, in particular on basis of SAP Netweaver

Service description : Application Management Services (AMS)

SLA based Application Support for all SAP products to resolve application faults and to assist users following ITIL best practices in terms of Incident Management, Request Fulfilment, Problem Management and Change Management (minor and emergency change requests).

The service includes in detail:

- We start with efficient, well-structured organizational setup and knowledge transfer to ensure high-quality and SLA from the very beginning through our custom-tailored transition service
- Experienced SAP application consultants are involved for highest quality issue resolution:

- Remedying application faults, e.g. due to incorrect master data or customizing/ configuration settings and
- Supporting users in terms of handling and information issues

- All service processes we provide are ITIL based
- Local and global AMS service delivery is efficiently coordinated accordingly to customer support demand and individual requirements through our professional service delivery management.

SAP AMS does not have a one-size-fits-all scenario. Each company's needs are unique when it comes to SAP applications and their interplay with each other and third-party systems. However, the following end-to-end services are required as a minimum for companies and IT departments to deliver outcomes.

Application Support

- ✓ User Support
- ✓ Service Desk
- ✓ Event Management
- ✓ Service Request Fulfillment
- ✓ Incident Management
- ✓ Problem Management
- ✓ Change Request Management
- ✓ Application Stabilisation & Hypercare

Value-Add Application Management

- ✓ Functional Monitoring
- ✓ Testing
- ✓ Release Management
- ✓ Deployment Management
- ✓ Upgrades & EHP installations
- ✓ Feature Implementation

Service Management

- ✓ Proactive Coordination of all Managed Services
- ✓ Service-Level Management and Reporting
- ✓ Continuous Service Improvement
- ✓ SAP COE Consulting

Continuous Improvement & Innovation

- ✓ Idea & Innovation Management
- ✓ Business Value Creation, Innovation & Automation
- ✓ Multi-Provider Management

Additionally, we provide **advisory services**, e.g. guidance on strategic managed service topics, future product roadmaps and functional / technical improvements and **service delivery management**, means proactive coordination of all aspects of a managed service delivery towards the customer.

(2) Data Subjects affected by the Processing

- Customers (employees of customer as well as possible end- customers affected by the use of the service by the customer)
- Suppliers
- Service providers (e.g. external consultants, external trainers, external sales agents, distributors)
- Strategic partners

(3) Data Types

The types of data processed for the performance of the service are:

- Personal master data/personal identification data (e.g. name, address, job title, company affiliation)
- Electronic identification data (e.g. IP address, electronic signature, connection/log data, cookies)
- Communication data (e.g. telephone, e-mail, PIN, password, ports, login)
- Pictures (photos, films, etc.)

(4) Frequency of the Transfer

Personal Data can be transferred during the entire contractual period of the service(s).

(5) Deletion Period

Personal Data can be retained for the duration of the service contract.

Appendix 2: Technical and Organizational Measures to ensure the Security of the Transferred Personal Data (Managed Services)

1. **Scope of Applicability**

   The following technical and organizational measures must be complied with by the service provider. Items marked with *"only MCS"* shall only apply in case of a Managed Cloud Service contract.

2. **Confidentiality**

   Measures to implement the confidentiality requirement include, among other things, measures for entry, access or admission control. In this context, the following technical and organizational measures on the part of the Contractor are intended to ensure an appropriate level of security for Personal Data, including protection against unauthorized or improper processing and against accidental loss, destruction or damage.

   a.) Entry control

   Measures to prevent unauthorized persons from gaining access to data processing equipment with which Personal Data is processed and used.

   The following measures are implemented by the Contractor:

   - Physical building protection
   - Logging of visitors
   - Locking system with coded locks
   - Burglar alarm system
   - Automatic access control system
   - Key rule (key list)
   - Security doors and locks
   - Careful selection of cleaning personnel
   - Chip card/transponder locking system
   - Use of carefully selected security personnel
   - Obligation to carry authorization cards
   - Light barriers/motion detectors
   - Manual locking system
   - Identity checks by gatekeepers/reception staff
   - Function- and role-based access authorizations

   b.) Access control

   Measures to prevent unauthorized parties from using data processing systems. The following measures have been implemented by the Contractor in addition to the aforementioned controls:

   - 2-factor authentication
   - Key control (key output, etc.)

- Authentication via user name/ password
- Secure storage of data carriers (backup tapes, hard disks, etc.)
- Authentication via biometric methods *(only MCS Data Center)*
- Use of a shredder
- Careful selection of transport personnel and vehicles
- Use of antimalware software
- Destruction of data carriers by certified disposal companies
- Use of a hardware firewall
- Destruction of paper documents by certified waste disposal companies
- Use of an identity management system
- Use of a software firewall
- Encryption at directory and file levels
- Encryption of data carriers in laptops/notebooks
- Use of lockable disposal containers for paper, files and data carriers
- Encryption of mobile data carriers (USB sticks, CDs/DVDs etc.)
- Encryption of smartphone content
- Use of VPN technology
- Use of secure transport containers/packaging for physical transport
- Creation of user profiles
- Network and network area concept
- Assignment of user profiles to IT systems
- Emergency management for Contractors (e.g. multi-shift operation, on-call duty, substitute regulation)*
- Assignment of user rights from a function and role-based perspective

c.) Admission control

Measures to ensure that those authorized to use a data processing system can only access data they are entitled to access, and that Personal Data cannot be read, copied, changed or removed without authorization during processing and use or after storage.

The following measures have been implemented by the Contractor in addition to the aforementioned controls:

- Number of administrators limited to a minimum
- Logging of accesses to applications, especially when entering, modifying and deleting data
- Function and role-based authorization concept
- Management of access authorizations in compliance with the separation of functions and the principle of dual control
- Records of the destruction of paper, files and data carriers

d.) Separation control

Measures ensuring that data collected for different purposes can be processed separately.

The following measures have been implemented by the Contractor in addition to the aforementioned controls:

- For pseudonymized data: Separation of the association file and storage on a separate, secure IT system
- Physically separated storage on separate systems or data carriers
- Definition of database rights
- Providing the data records with purpose attributes/data fields
- Logical client separation (software-side)
- Separation of productive- , test- and development systems

e.) Pseudonymization

Pseudonymization is the processing of Personal Data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to corresponding technical and organizational measures.

- Selection of a suitable method for pseudonymization using the latest technology
- The pseudonymization requirement is a central component of the Contractor's data protection concept

f.) Encryption

Encryption is intended to prevent access to Personal Data by unauthorized persons or provide warning of the same (e.g. hacker attacks or espionage). Encryption refers to the process of converting data into a form known as ciphertext, which is difficult for unauthorized persons to understand.

- Selection of a suitable method for encryption using the latest technology
- Regular checking of encryption methods for security loopholes and updating of relevant software as required
- Email encryption
- Deletion concept for sent encrypted files
- Use of an encryption method corresponding to the data protection concept
- Encryption on directory and file level
- Processes for managing and protecting cryptographic information (authorization concept for internal and external employees)
- Encryption of smart devices
- Encryption of mass storage in Laptops and Notebooks
- Encryption of portable storage devices (USB sticks, hard drives, CD/DVD, etc.)

3. Integrity

Measures to implement the integrity requirement firstly include those within the scope of input control, but secondly, also those that generally help protect against unauthorized or unlawful processing, destruction or unintentional damage. In this context, the following technical and organizational measures on the part of the Contractor are intended to ensure the integrity of Personal Data:

a.) Transfer control

Measures to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport or storage on data media, and that the intended recipients of the data transmitted using data transmission facilities can be verified and determined.

The following measures have been implemented by the Contractor in addition to the aforementioned controls:

- Obligation of employees to prohibit the betrayal of business and trade secrets
- Email encryption
- Transfer of data in anonymous or pseudonymized form
- Setting up dedicated lines or VPN tunnels
- Creation of an overview of periodic polling and transmission operations
- The transfer of the Client's data is only carried out in Agreement with the Client and to the recipient it has specified. All employees of the Contractor are obliged to maintain confidentiality and data secrecy as part of their employment contract with the Contractor, and have been informed in writing of the legal consequences in the event of any infringement.

b.) Input control

Measures to ensure scope to subsequently verify and determine whether and by whom data have been entered, modified or removed in data processing systems.

The following measures have been implemented by the Contractor in addition to the aforementioned controls:

- Storage of forms from which data has been transferred to automated processing operations
- Logging of input, modification and deletion of data
- Creation of an overview showing which applications can be used to enter, change and delete which data.
- Assignment of rights for entering, modifying and deleting data on the basis of an authorization concept
- Traceability of the input, modification and deletion of data by individual user names (not user groups)
- The employees of the Contractor only create, change or delete data or datasets of the Client in response to individual, written instructions and within the scope of incident and change management in accordance with ISO/IEC 20000-1:2011. During this process, both the

clearance of the Client and the changes made are documented. An overview of the changes made is included in the monthly reports to the Client.

4. Availability and resilience of systems

Measures to ensure that, data and IT systems are available and can be used by authorized persons when required. Unauthorized interruptions, e.g. due to server failure or failure of communication media, constitute an attack on availability. These measures are also designed to ensure that systems on which Personal Data is stored can withstand a certain degree of stress and are monitored regularly, and also that an appropriate emergency management system has been established for the same.

a.) Availability control

Measures to ensure that data is protected against accidental destruction or loss.

The following measures have been implemented by the Contractor in addition to the aforementioned controls:

- Alarm message in the event of unauthorized access to server rooms *(only MCS Data Center)*
- Emergency manual
- Storage of data backups in a secure and outsourced location *(only MCS Data Center)*
- Emergency plan
- Fire and smoke detection systems
- Regulations governing the availability and reliability of the Contractor's performance
- Fire extinguishing systems in server rooms *(only MCS Data Center)*
- Surge protection concept in server rooms *(only MCS Data Center)*
- Measures to prevent water ingress in server rooms *(only MCS Data Center)*
- Devices for monitoring temperature and humidity in server rooms *(only MCS Data Center)*
- Testing of data recovery *(only MCS Data Center)*
- Cooling technology in server rooms/racks *(only MCS Data Center)*
- Uninterruptible power supply (UPS) *(only MCS Data Center)*
- Concept for the backup, restoration and recovery of data by the Contractor *(only MCS Data Center)*
- Concept for the archiving of data by the Contractor
- Details of the availability agreed between Client and Contractor and the backup, restoration and recovery measures are described in the underlying Service Contract

b.) Resilience of the Systems and Services

This includes measures used by the contractor for monitoring the systems and to identify and avoid heavy system load at an early stage

- Setting the stress limit for the respective systems above the requisite minimum. For further details see 3 a) “Availability control”. (only MCS Data Center)

- Individual details of the recoverability agreed between the Client and Contractor are described in the underlying Service Contract.

5. Procedures for regular review, assessment and evaluation

a.) Organizational control

Measures for the organization of the internal organization that meet the special requirements of data protection.

- Data protection management
- Activities of employees in job, function and role descriptions
- Notification procedures
- Incident and Security Incident response management
- Information procedures
- Disposal concept
- Separation of functions and responsibility between data owners and processors
- Training of employees in dealing with the data protection law
- Appointment of a data protection officer; defining and announcing of tasks
- Data security policy
- Guideline on hardware and software to be used, including investment and approval procedures
- Creation and maintenance of a list of processing activities for processors
- information security that describes the security controls for the information systems and the rules of behavior for individuals accessing the information systems
- Concept for information classification that ensures properly and consistently document classification
- Risk management as well as information security in projects
- Risk management program that identifies, manages and follows-up on information security risks
- Regularly policy review (at least yearly)
- Existing vulnerability management program that identifies, manages and tracks vulnerabilities

b.) Order control

Measures to ensure that Personal Data processed on behalf of the Contract can only be processed in accordance with the Clients instructions.

The following measures are implemented by the Client and Contractor in addition to the aforementioned checks:

- Selection of Client by the Contractor with the application of due diligence (particularly concerning data security) Checking of the Contractor at the Clients request by a data protection officer

- Checking of the Contractors documentation and security measures by the Clients prior to data processing
- Written instructions issued to the Contractor by the Client in accordance with this Agreement (e.g. as part of an Agreement for commissioned data processing)
- Agreed-upon effective control rights of the Client against the Contractor
- Ensuring the destruction of data by the Contractor and the Client on completion of the order