intershop

Data Processing Agreement (Cloud)

- hereinafter referred to as „Agreement"-

according to Art. 28 para. 3 General Data Protection Regulation (GDPR)

1. Subject Matter and Duration of the Agreement

1.1 Subject Matter of this Agreement is the provisioning of hosting and cloud services in the context of the agreement closed with Controller (Intershop Communications AG) on (hereinafter also „Main Agreement") and additional commissions in the context of the Main Agreement and this Agreement respectively relating to data protection.

1.2 Subject matter of this Agreement is **not** an original use or processing of personal data by Processor (Customer). In the course of provision of services by Processor as central IT service provider in the field of hosting, support and administration of Controller's server systems, the provision of development services, the performance of business management activities and storage of data of Controller, however, access to personal data cannot be excluded or access may be permitted upon express commission. Controller shall remain the responsible authority in the meaning of data protection laws („master of data").

1.3 Term and termination of this Agreement shall depend on terms and conditions of the Main Agreement relating to term and termination. Termination of Main Agreement shall automatically include termination of this Agreement. A separate termination of this Agreement shall be excluded.

2. Clarification of the Content of the Agreement: Scope, Nature and Purpose of Processing, the Categories of Personal Data and Categories of Data Subjects

2.1 Scope, type and purpose of access to Controller's data by Processor can be derived from the specifications of the individual order confirmations of Processor relating to hosting services. Summarizing, there will be access in the following instances:

- Hosting virtual computers, network and storage components as well as the applications operated there (such as Web, App, Solr, database, backup, transfer servers or storage services);
- Technical administration of systems and related services;
- Activities in the context of Application Management (e.g. in the course of proactive monitoring);
- Technical analysis of requests and the implementation of agreed services (e.g. migration of customer data,...)
- Execution of quality assurance measures
- Execution of agreed services of business management activities

For the purpose of fulfilling this Agreement, access to data set forth in item 2.2 below by Processor cannot be excluded or access will be made according to item 1.2 above respectively.

2.2 Categories of Data

Data categories relating to commissioned services as regards customers and their final customers, suppliers, business partners and employees of Controller are as follows:

- Master data
- Contact details
- Contract data
- E-Commerce data
- Contract control data

- Log files

2.3 Categories of Data Subjects

Categories of data subjects affected by handling of their data in the context of this Commission shall include:

- Customers and potential customers of Controller (end users);
- Employees, suppliers and business partners of Controller.

To the extent the list included in item 2.2 and 2.3 above needs to be adjusted, the Parties shall agree on such adjustment through an annex to this Commission.

3. Technical and Organizational Measures

3.1 The Processor shall design its internal company organization in such a way that it meets the special requirements of data protection. The Processor has to produce the security according to Art. 28 para. 3 lit. c. and Art. 32 GDPR, especially in connection with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk in terms of confidentiality, integrity, availability and system resilience. The state of the art, implementation costs and the nature, scope and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR shall be taken into account. For this purpose, the Processor shall in particular take the technical and organizational measures defined in **Annex 1** to adequately secure the personal data against misuse and loss.

3.2 The Parties are in agreement that any technical and organizational measures are subject to technical progress and further developments. Insofar the Processor shall be permitted to implement adequate alternative measures. Processor shall notify Controller in due time about it and shall ensure that an anticipated measure does not fall below the safety level of the agreed measure. Any major changes shall be discussed and agreed in advance with Controller, and are to be documented by Processor.

4. Correction, Blocking, Deletion of Data

4.1 The rights of the data subjects affected by the handling of data at the Processor's premises, in particular with regard to correction, restriction and deletion, shall be asserted against the Controller. The Controller is solely responsible for safeguarding these rights. The Processor may not correct, delete or restrict the processing of personal data on its own initiative, but only in accordance with the documented instructions of the Controller. The Processor shall implement the instructions of the Controller without delay, unless the Processor has a legal obligation to store personal data.

4.2 Processor shall be obligated to immediately forward to Controller any requests of data subjects affected or supervisory authorities addressed to Processor in the context of its commissioning in order to ensure proper processing of such requests. Processor shall be under no obligation to independently decide about such requests without having discussed it with Controller.

4.3 Processor shall, at the Controller's request and to the best of its ability, assist the Controller in fulfilling the rights of the data subjects affected, in particular with regard to the right to be forgotten and the right to data portability. The correction, restriction and deletion of the data concerned during provision of services shall be made by Processor on behalf of Controller.

4.4 The Processor shall be entitled to compensation for assisting the Controller in safeguarding the rights of the data subjects concerned. Unless otherwise agreed, this shall be based on the time required and the remuneration rates of the Processor's current price list.

5. Processor's Duties

5.1 The Processor collects, processes and uses personal data within the framework of the Main Agreement as well as the specific instructions of the Controller.

5.2 In connection with the fulfilment of the obligation to notify the Controller in accordance with Art. 33 and 34 GDPR, the Processor shall immediately report to the Controller in writing in all cases in which the Processor or the persons or sub-contractors employed by the Processor have violated any regulations for the protection of the Controller's personal data or the stipulations made in this Agreement. This shall also apply in the event of the loss or unlawful transmission or knowledge of personal data and in the event of serious disruptions to the course of business, suspicion of other violations against regulations for the protection of personal data or other irregularities in dealing with Controller's personal. This also applies to the case of control actions and measures of the supervisory authority pursuant to Art. 58 GDPR. This shall also apply in so far as a competent supervisory authority carries out an investigation at the Processor's premises in accordance with Art. 82, 83 GDPR.

5.3 The Processor shall inform the Controller without delay of any control actions and measures taken by the supervisory authority insofar as they relate to this Agreement. This shall also apply to the extent that a competent supervisory authority carries out an investigation in the course of administrative offences or criminal proceedings with regard to the processing of personal data during the order processing by the Processor.

5.4 Insofar as the Controller, for its part, is subject to a control by the supervisory authority, an administrative offence or criminal procedure, a liability claim of a data subject affected or a third party or any other claim in connection with order processing by the Processor, it shall support the Controller to the best of its ability.

5.5 Taking into account the nature of the processing and the information at its disposal, the Processor shall assist the Controller in complying with the statutory obligations set out in Art. 32 to 36 GDPR. These include among others

a. ensuring an adequate level of protection by means of technical and organizational measures which take into account the context and purposes of processing as well as the predicted likelihood and severity of a possible breach of the law due to security gaps and which enable an immediate detection of relevant infringement events,

b. the obligation to report any violations of personal data to the Controller without delay,

c. the obligation to support the Controller within the scope of its obligation to inform the data subjects affected and to provide it with all relevant information without delay in this connection,

d. assisting the Controller in its data protection impact assessment,

e. assisting the Controller in the context of prior consultations with the supervisory authority.

For support services that are not due to the Processor's malpractice, the Processors may claim compensation for such services. Unless otherwise agreed, this shall be based on the time required and the remuneration rates of the Processor's current price list.

5.6 The Controller is entitled at any time to demand correction, deletion and blocking of personal data.

5.7 The Processor documents the data processing and provides the Controller with the documentation on request.

5.8 The Processor undertakes to maintain a record of processing activities in accordance with Art. 30 para. 2 GDPR. The record shall be kept in writing or in an electronic format and shall be presented to the Controller and/or his data protection officer at any time on request.

6. Confidentiality

6.1 The Processor warrants that the persons authorized to process personal data have undertaken to maintain data secrecy and confidentiality or are subject to an appropriate statutory duty of confidentiality. The Processor has informed the employees employed by it as a precautionary measure about the observance of telecommunications secrecy pursuant to § 88 TKG (German Telecommunications Act).

6.2 It shall be ensured that the obligation to maintain data secrecy and confidentiality shall continue even after termination of this Agreement.

7. Data Protection Officer

7.1 The Processor has appointed a data protection officer. This is at the time of conclusion of the contract:

Mr. Dr. Uwe Schläger
datenschutz nord GmbH
e-mail: Datenschutzbeauftragter@Intershop.de

7.2 The Processor shall notify the Controller immediately in writing of any dismissal or reappointment of the Data Protection Officer.

8. Transfer to non-EEA countries

8.1 Subject to the provisions of clause 9.4, 9.5 and 9.6, the collection, processing and use of personal data by the Processor shall be restricted to a Member State of the European Union or a contracting state of the Agreement on the European Economic Area. The transfer of personal data by the Processor to an entity located outside the EEA, i. e. a company with its registered office outside the EEA, is only possible subject to compliance with the statutory provisions, the prior information of the Controller and the lack of any objection. Exceptions to this are only possible in the cases mentioned in Art. 28 para. 3 lit. a GDPR under the additional conditions mentioned there.

8.2 If, under the applicable law of a Member State or the European Union, the Processor is obliged to transfer data to an entity located outside the EEA, the Processor shall notify the Controller prior to processing in accordance with its obligation under Article 28 para 3 lit. a GDPR, insofar as the applicable law does not prohibit such notification on account of an important public interest.

8.3 The use of Microsoft (Azure Services), Atlassian (Cloud Services Confluence) and DataDog (Monitoring Services) as subcontractors within the meaning of Section 9 is expressly referred to.

9. Sub-Contracting Relationships

9.1 For the purposes of this provision, sub-contracting relationships shall mean those services which relate directly to the provision of the main service. Services which are rendered by third party companies to Processor as additional services in order to support Processor in fulfilling its duties shall not be considered as sub-contracting relationships. These services shall include, e.g. telecommunication services, maintenance and user services, cleaning services, auditors or disposal of data carriers. However, in the event of additional services provided by third parties, Processor shall be obligated to arrange for appropriate and legally sufficient contractual stipulations in order to ensure protection and safety of Controller's data.

9.2 The Contractor may engage sub-contractors (additional processors) to provide certain or supporting services to the Contractor.

The Controller agrees that the Processor shall use affiliated companies of the Processor for the fulfilment of its contractually agreed services or sub-contract other third parties with services if the Processor concludes a contractual agreement with the sub-contractor in accordance with Art. 28 para. 2-4 GDPR, the level of protection of which is at least

equivalent to that of this Agreement. The aforementioned authorizations constitute the prior general written consent of the Controller to the subcontracting of the processing of Controller´s Customer Data and Personal Data by the Processor, if such general consent is required under the Standard Contractual Clauses or the provisions of the GDPR.

9.3 The Processor may occasionally engage new sub-contractors. The Processor shall inform the Controller of any new sub-contractor at least 1 month before the sub-contractor gains access to Controller´s Data (by providing a mechanism to notify the Controller of such update).

Controller may reasonably object to Processor's use of a new sub-contractor (e.g., if providing personal data to the sub-contractor violates applicable data protection laws or weakens the protection of such personal data) by notifying Processor accordingly in writing without undue delay, but no later than 14 calendar days after Controller becomes aware of such change. Such notice shall be sent to the e-mail address Datenschutzbeauftragter@intershop.de, shall include the date on which the Controller became aware of the new sub-contractor and shall set forth the reasonable grounds for the objection. In the event that Controller objects to a new sub-contractor in accordance with the foregoing, Processor shall use commercially reasonable efforts to provide Controller with a modification to Processor's Services or recommend a commercially reasonable modification to Processor's configuration or use of the services to avoid the processing of Personal Data by the objected-to new sub-contractor without cause.

If the Processor is unable to provide such a change within a reasonable period of time, which shall be 14 calendar days from the date on which the Processor has received written notice from the Controller, each party shall only be entitled to terminate the Main Agreement if the services contractually owed under the Main Agreement can no longer be provided in their essential components.

9.4 Microsoft Azure: The Controller hereby approves use of Microsoft (Microsoft Ireland Operations Ltd., hereinafter "Microsoft") as sub-contractor under the condition of a contractual agreement in accordance with Art. 28 para. 2-4 GDPR.

a. Processor may contract infrastructure and platform services (hereinafter “Microsoft Services”). Currently, the Processer uses the following Microsoft Services: Compute, Network, Storage and related DevOps Tools.

b. The use of the Microsoft Services is carried out by the Processor in accordance with the Microsoft Terms of Use and Security Measures attached to this Agreement as Annex (Microsoft Terms and Conditions for Online Services).

c. Microsoft and its controlled subsidiaries have agreed on standard contractual clauses to ensure an appropriate level of protection. Refer to Annex 2 for details.

d. The Processor has concluded a contract with Microsoft that satisfies the substantive requirements for data processing agreements in accordance with Art. 28 para. 3 GDPR. To the extent necessary, the Controller shall authorize the Processor to agree on its behalf with Microsoft on the applicability of the EU standard contractual clauses.

9.5 Atlassian: The Controller hereby approves use of Atlassian (Atlassian PTY Ltd, Atlassian, Inc., Trello Inc., Dogwood Labs, Inc., OpsGenie, Inc., Agile Craft LLC and Halp Inc., which are all Atlassian entities, "Atlassian") as a sub-contractor under the condition of a contractual agreement in accordance with Art. 28 para. 2-4 GDPR.

a. Processor may contract cloud services from Atlassian for the use of Confluence, a collaboration tool for knowledge management and project collaboration (hereinafter "Atlassian-Services"). Processor currently uses the following services from Atlassian: cloud services for Confluence tool for knowledge management and project collaboration.

b. The Processor has concluded a contract with Atlassian that meets the content requirements for commissioned processing agreements pursuant to Article 28 para. 3 GDPR. To the extent necessary, the Controller authorizes the Processor to agree on its behalf with Atlassian on the applicability of the EU standard contractual clauses.

9.6 DataDog: The Controller hereby approves use of DataDog (DataDog, Inc., 620 8th Avenue, 45th Floor, New York, NY 10018-1741 USA, „DataDog") as a sub-contractor under the condition of a contractual agreement in accordance with Art. 28 para. 2-4 GDPR.

a. Processor may contract monitoring services from DataDog (hereinafter "DataDog Services"). Processor currently uses the following services from DataDog: monitoring and log analytics.

b. The Processor has concluded a contract with DataDog that meets the content requirements for commissioned processing agreements pursuant to Article 28 para. 3 GDPR. To the extent necessary, the Controller authorizes the Processor to agree on its behalf with DataDog on the applicability of the EU standard contractual clauses.

10. Control Rights of the Controller

10.1 Prior to the start of data processing by the Processor and then regularly, at its own expense, the Controller shall have the right to carry out an order control in consultation with the Processor with regard to the data processing to be carried out by the Processor or to have it carried out by inspectors to be nominated in individual cases by the Controller, provided that the Controller or the nominated inspectors undertake to conclude a non-disclosure agreement with the Processor or its sub-contractors, unless the nominated inspectors are subject to professional confidentiality obligations. If the inspector ordered by the Controller is in competition with the Processor, the Processor has the right to object. After prior notification in good time (usually at least 2 weeks in advance) the Controller shall have the right to verify compliance with this Agreement by the Processor by carrying out random samples in the Processor's business operations during normal business hours without disrupting the course of operations. In cases where there is a reasonable suspicion of data protection violations or other disruptions, prior notification is not required. The Controller may normally carry out one control per calendar year. This does not affect the Controller's right to carry out further controls in the event of special occurrences. The Processor undertakes to provide the Controller, on request, with the information necessary to safeguard its obligation to control its commissioning and to make the corresponding evidence available to the extent possible.

10.2 The Processor shall ensure that the Controller can convince itself of the Processor's compliance with its obligations pursuant to Article 28 GDPR. Upon request, the Processor shall provide evidence of the implementation of the technical and organizational measures taken.

10.3 The Processor undertakes to provide the Controller, on request, with the information and evidence necessary to safeguard the Controller's obligation to check the commissioning and, if available, to provide evidence. Evidence of the implementation of suitable measures can also be provided by submitting current certificates and reports from independent auditors (accountants, auditors, data protection officers, IT security department, etc.). This shall also apply in so far as the Processor carries out the control of its sub-contractors on behalf of the Controller.

10.4. The provisions of clause 9 shall apply to the services provided by sub-contractors.

10.5 If the Controller identifies defects in compliance with technical and organizational measures within the scope of the order control, the Processor shall remedy the defects without delay. The Processor shall bear the costs necessary to remedy the defect.

11. Supervisory Rights of Controller

11.1 The Processor collects, processes and uses personal data on behalf of and on instructions from the Controller for the fulfilment of its obligations under the Main Agreement. Within the scope of this Agreement, the Controller is solely responsible for complying with the statutory provisions of the data protection laws, in particular for the lawfulness of the data transfer to the Processor and for the lawfulness of data processing ("Controller" within the meaning of Art. 4 No. 7 GDPR).

11.2 The handling of the data takes place exclusively within the framework of the agreements made. The Controller is entitled to issue instructions on the type and scope of data processing with regard to the implementation of data protection requirements, even during the assignment (individual instructions). In each case, the instructions must be given in writing and may not contradict the contractually agreed performance by the Processor. Individual instructions which deviate from the stipulations of this Agreement or contain additional requirements require the prior consent of the Processor.

11.3 Instructions of the Controller are to be documented by the Processor.

11.4 If the Processor is of the opinion that any instructions given by the Controller are contrary to GDPR or other data protection provisions of the European Union or the Member States, it shall inform the Controller thereof in writing. In such cases, the Processor shall be entitled to suspend the execution of the instruction until the Controller confirms or modifies the instruction. However, legal advice and/or legal research by the Processor is not owed.

11.5 The Processor shall not use the data for any other purposes and in particular shall not be entitled to pass on data to third parties. Copies and duplicates will not be made without the Controller`s knowledge. Copies are excluded from this, insofar as they are necessary to guarantee the proper performance of services.

12. Deletion and Return of Personal Data

12.1 At the end of the Main Agreement, the Processor shall release the data concerned to the Controller or delete them on request in accordance with the state of the art, unless otherwise agreed in individual cases or unless the Processor is legally obliged to keep such data for further storage; however, such data shall then be blocked and stored in accordance with the provisions of this Agreement. In any case, the data will be deleted no later than 90 days after expiry or termination of the Main Agreement. The deletion log shall be submitted on request.

12.2 There is no data medium exchange between the Parties to this Agreement. In this respect, a return is not to be regulated here. Otherwise, the Parties shall agree separately.

12.3 The Processor has no right of retention of the contractual data.

12.4 The Processor shall keep documentation that serves as proof of proper data processing in accordance with the respective retention periods beyond the end of the contract. It can hand them over to the Processor at the end of the contract to relieve himself. The Processor shall maintain silence about the data of the Controller even after the end of the order.

13. Liability

A liability provision agreed between the parties in the service contract (Main Agreement) shall also apply to commissioned data processing, unless expressly agreed otherwise. For the rest Art. 82 GDPR shall apply.

14 Final Provisions

14.1 The parties agree that this Data Processing Agreement supersedes and replaces all previous data processing agreements between the parties.

14.2 Should the Controller's data be endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Processor shall inform the Controller thereof without delay. The Processor shall inform all persons responsible in this context without delay that the sovereignty and ownership of the data shall lie exclusively with the Controller as the "Controller" within the meaning of the GDPR.

14.3 Insofar as costs are incurred within the scope of this order, in particular in connection with supporting actions, the surrender or deletion of data, they shall be borne by the Controller.

14.4 In the event of changes to the actual arrangement of the service relationships between the Parties, the Parties shall adapt the annexes accordingly and exchange them by mutual agreement. With the signing of the amended annex by the Parties, it becomes effective and replaces the existing annex.

14.5 Changes or additions to this Agreement must be made in writing. This applies accordingly to the amendment or cancellation of this written form requirement.

14. 6 Changes in the person or the competence of the authorized persons must be communicated to the other Party immediately in writing.

14.7 German law applies, the place of jurisdiction is Jena.

14.8 This Agreement has the following elements:

- Text of the present Agreement
- Annex 1 Technical and Organizational Measures pursuant to Art. 32 GDPR
- Annex 2 Microsoft Terms and Conditions for Online Services and Standard Contractual Clauses (for Global Cloud)
- Main Agreement

In the event of ambiguities and/or contradictions between the individual documents or parts of the contract, the components shall apply in descending order.

14.9 Should individual provisions of this Agreement be or become invalid, the validity of the remaining provisions of this agreement shall remain unaffected. The ineffective provision shall be replaced by an effective provision which comes as close as possible to the economic content of the ineffective provision. The same applies in the case of loopholes.

Annex 1: Technical and Organizational Measures pursuant to Art. 32 GDPR

Annex 2: Microsoft Terms and Conditions for Online Services and Standard Contractual Clauses (for Global Cloud)

Annex 1 Technical and Organizational Measures

According to Art. 32 para. 1 Controller (Art. 30 para. 1 lit. g) and Processor (Art. 30 para. 2 lit. d)

This Annex describes technical and organizational safety measures on the Jena site of INTERSHOP. For storage of data in the data processing centre item 9.3 shall apply.

Equipment access control

Deny unauthorized persons access to processing equipment used for processing:

- Visitor's stay only in the presence of employees
- Authentication by user name & password or key
- Automatic door closing and acoustic open signal for entrance doors
- Burglar-resistant windows
- Use of firewalls
- Use of VPN
- Narrow limitation and restriction of authorized users (need-to-know and least-privilege principle)
- Determination of persons entitled to access
- separate systems per customer (virtual private cloud)
- password policy
- Data protection and IT security guidelines
- Temporary blocking of access (e.g. more than three unsuccessful login attempts)
- Unique User IDs, login with a general administrator account is restricted
- Subdivision into safety zones, restricted areas
- Maintenance work by external service providers only after prior registration
- Central user administration incl. role and rights system
- Central key management

Data media control

Prevent the unauthorized reading, copying, modification or erasure of data media:

- Disposal of data mediums only to authorized persons
- Authentication by user name & password or key
- Narrow limitation and restriction of authorized users (need-to-know and least-privilege principle)
- User identification and authorization check
- Inventory of data mediums
- Proper destruction of data carriers and data protection-compatible data carrier disposal
- Organizational separation of development, operations and management
- Data protection and IT security guidelines
- Ensuring the destruction of data after completion of the order
- Verification of the storage of data carriers

Storage control

prevent the unauthorized input of personal data and the unauthorized inspection, modification or deletion of stored personal data

- Narrow limitation and restriction of authorized users (need-to-know and least-privilege principle)
- User identification and authorization check
- Proper destruction of data carriers and data protection-compatible data carrier disposal
- Data protection and IT security guidelines
- Encryption of mobile data mediums

User control

Prevent the use of automated processing systems by unauthorized persons using data communication equipment:

- Narrow limitation and restriction of authorized users (need-to-know and least-privilege principle)
- network access control
- Data protection and IT security guidelines
- Unique User IDs, login with a general administrator account is restricted
- Central user administration incl. role and rights system

Data access control

Ensure that persons authorized to use an automated processing system have access only to the personal data covered by their access authorization:

- Disposal of data mediums only to authorized persons
- Authentication by user name & password or key
- Use of virus scanners
- Narrow limitation and restriction of authorized users (need-to-know and least-privilege principle)
- separate systems per customer (virtual private cloud)
- User identification and authorization check
- Proper destruction of data carriers and data protection-compatible data carrier disposal
- Logging of data entry, modification and deletion
- Data protection and IT security guidelines
- Unique User IDs, login with a general administrator account is restricted
- Central key management

Communication control

Ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment:

- Use of e-mail encryption at relevant points
- Use of VPN
- Logging of transmissions
- Data protection and IT security guidelines
- Training and sensitization of employees

Input control

Ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input:

- User identification and authorization check
- Logging of data entry, modification and deletion
- Data protection and IT security guidelines
- Unique User IDs, login with a general administrator account is restricted

Transport control

Ensure that the confidentiality and integrity of personal data are protected during transfers of personal data or during transport of data media:

- Disposal of data mediums only to authorized persons
- Use of e-mail encryption at relevant points
- Use of VPN
- Data protection and IT security guidelines

Recoverability

Ensure that installed systems may, in the case of interruption, be restored:

- Redundant design of the productive database
- Regular replication of the database (several times within one hour)
- Data protection and IT security guidelines
- Random restore tests
- Daily database backup

Reliability

Ensure that all system functions perform and that the appearance of faults in the functions is reported:

- Active update and patch management
- Proactive monitoring of the customer environment
- Data protection and IT security guidelines
- Random restore tests

Integrity

Ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system:

- Active update and patch management
- Data protection management system (internal audits, risk management)
- separate systems per customer (virtual private cloud)
- Proper destruction of data carriers and data protection-compatible data carrier disposal
- "Regular replication of the database
- (several times within one hour) "
- Data protection and IT security guidelines
- Training and sensitization of employees
- Random restore tests
- Daily database backup

Processing control

Ensure that personal data processed on behalf of the controller can only be processed in compliance with the controller's instructions:

- Selection of subcontractors with due diligence in particular with regard to information security
- supervision rights
- Data protection and IT security guidelines
- Ensuring the destruction of data after completion of the order
- Obligation to comply with the data protection regulations of employees

Availability control

Ensure that personal data are protected against loss and destruction:

- Active update and patch management
- Use of firewalls
- Use of Load Balancer
- Use of virus scanners
- Fire and smoke detection systems
- Fire extinguishers in the rooms
- gas extinguishing system
- air conditioning
- no-smoking policy
- "Regular replication of the database
- (several times within one hour) "
- Data protection and IT security guidelines
- Daily database backup
- Comprehensive system monitoring
- Uninterruptible power supply (UPS)

Separability

Ensure that personal data collected for different purposes can be processed separately:

- Use of firewalls
- separate systems per customer (virtual private cloud)
- Organizational separation of development, operations and management
- Data protection and IT security guidelines
- Separation of test and production system
- Subdivision into safety zones, restricted areas
- Central user administration incl. role and rights system

Confidentiality

Protection against unauthorized disclosure of data:

- Pseudonymization of personal data in the context of tests on non-productive customer systems (pre-production, integration, development)
- Data protection and IT security guidelines
- Ensuring the destruction of data after completion of the order
- Encrypted transmission of personal data outside the customer environment

Procedures for regular review, assessment and evaluation of the effectiveness of technical and organizational measures

- Data protection management system (internal audits, risk management)
- incident management

Annex 2 Microsoft Terms

The use of the Microsoft Services is carried out by the Processor in accordance with the Microsoft Terms of Use and Security Measures, which are to be found under the following links:

- https://www.microsoft.com/licensing/terms/en-US/product/ForOnlineServices/EAEAS and
- https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS.