Contract terms for the licensing of cloud services

1. Object of agreement

1.1 The quality and specification of the cloud service is based on the respective program description and order confirmation.

1.2 The Provider shall provide the Customer the possibility to use the cloud service by remote access via Internet during the term of the contract. The required cloud service and computer performance as well as the required storage space for cloud software data shall be made available by the Provider or by a colocation center assigned by the Provider. The system area allocated to the Customer shall be protected against third-party access.

1.3 The Provider shall transfer the access data required for identification and authentication purposes which is required for the usage of the cloud service to the Customer. The Customer is not authorized to pass the access data to third parties, unless the third party is an additional user which has been authorized and registered by the Provider and that has been considered in the remuneration. The Customer shall be obliged to report additional users to the Provider before performing any activities so the adjustment of the remuneration can be conducted.

1.4 All other services of the Provider that are carried out by request of the Customer (in particular preparation for use, demonstration, education, training and consultation) will be charged separately according to the effort required.

2. Conditions for use

2.1 It is necessary for the Customer to have Internet access to use the cloud service. The Internet access of the customer is not part of this contract. The Customer shall bear sole responsibility for the operability of his Internet access (including transmission channels) as well as his own computer.

2.2 Further technical requirements for the use of the cloud service shall be published in the program description or the release notes of the cloud service.

3. Service Level

3.1 The Provider shall provide the cloud service with an availability of 99.5 % within the operational period. The operational period starts weekly on Sundays at 10:00 a.m. CET and-ends on the following Sunday at 4:00 a.m. CET with the result that a maintenance window is agreed between 4:00 a.m. CET

and 10:00 a.m. CET that shall not be deemed as a period of operation. Further excused downtimes shall not be included in the calculation of availability as long as the Provider has informed the Customer at least one (1) week in advance.

3.2 Availability shall be measured and calculated based on a calendar month. Availability shall be calculated using the following formula:

$$Value\ in\ percent = \frac{\Sigma\ Downtime\ during\ the\ operational\ period}{\Sigma\ \text{Service time} - \Sigma\ \text{Excused downtime}} \times 100$$

4. Removal of incidents of the cloud service

4.1 The Provider warrants that the cloud service meets the agreed specifications according to Section 1.1 within the operational period if applied as specified. Cloud service defects (hereinafter referred to as "incidents") shall be removed by the Provider within the reaction time defined in Section 4.2 et seq. after a corresponding notification of the incident by the Customer. The same shall apply for all other incidents of the potential usability of the cloud software.

4.2 The Provider shall accept incident reports by the Customer and assign them to the agreed incident categories. Based on this categorization, the agreed steps for analysis and removal of the incidents. Incident management shall not include any services associated with the use of cloud service in non-approved operational environments or with modifications of the cloud service implemented by the Customer or third parties.

4.3 During the operational period the Provider shall accept incident reports from the Customer and assign it with an identifier. On request of the Customer the Provider shall confirm the receipt of an incident report and provide the assigned identifier.

4.4 Unless otherwise agreed the Provider will assign the received incident reports to one of the following categories after an initial inspection:

4.4.1 **Major incident:** The incident is based on an error in the cloud service which makes it impossible or severely limited to use the cloud service. The Customer is not able to circumvent this issue in a reasonable way and is not able to execute unpostponable tasks as a result of the incident.

4.4.2 **Miscellaneous incidents:** The incident is based on an error in the cloud service, which significantly limits the use of the cloud service for the Customer without being a major incident.

4.4.3 **Miscellaneous reports:** Incident reports that cannot be classified into the categories of the Sections 4.4.1 and 4.4.2 shall be allocated to miscellaneous reports. The Provider shall treat miscellaneous reports according to the agreed conditions for this category.

4.5 In the case of reports of major incidents and miscellaneous incidents, the Provider shall immediately initiate appropriate measures corresponding to the circumstances communicated by the Customer in order to initially locate the cause of the incident. If the reported incident is not deemed as an error of the cloud service after the first analysis, the Provider shall immediately communicate this to the Customer. Otherwise, the Provider shall take appropriate measures to further analysis and eliminate the reported incident or - in the case of third-party components - communicate the incident report along with its analysis results to the seller or manufacturer of the components with the request for assistance. The Provider shall, within a reasonable deadline, provide the Customer with measures available to him in order to work around or remove the error of the cloud service, for example instructions for action. The Customer shall immediately take such measures in order to work around or remove incidents and again report any remaining incidents to the Provider during use of the software without undue delay. The Customer shall only claim for defects if the reported defects are reproducible or otherwise traceable by the Customer.

5. Contact center (Hotline)

5.1 The Provider shall set up a contact point for the Customer (Hotline). The Hotline shall process the requests of the Customer in regard with the technical operating requirements and conditions of the cloud service as well as the specific functional aspects. The Hotline shall not provide any services that are related to the use of cloud service in non-approved operational environments or to changes of the cloud service which has been conducted by the Customer or a third party.

5.2 For the receipt and processing of requests by the Provider it is required that the Customer names the members of his staff which are technically and professionally qualified and have been maintained internally with the processing of requests of the users of the cloud service to the provider. The Customer shall be obliged to place requests via the Hotline exclusively through the staff members that have been named to the provider and to use only the forms which have been made available by the Provider. The hotline shall accept these requests via E-mail and in case of Major Incidents also via phone call.

5.3 The hotline shall process proper requests during its normal course of business and answer them as far as possible. The Hotline has the possibility to refer to documentations which are already available for the Customer and to other training materials for the cloud service.

5.4 If it is not possible to either answer the request in general or to answer it in a timely manner via the Hotline the Provider shall forward the request for processing unless expressly agreed. This particularly

takes effect for requests concerning components of the cloud service that has not been produced by the Provider.

5.5 Further services of the Hotline, such as different response times and response deadlines as well as on-call services or on-site operations of the Provider shall be expressively agreed in advance.

6. Term of contract

6.1 The term of contract shall begin with the submission of the access data for the cloud service to the Customer. The term of the Contract shall be (1) year and shall be extended automatically by (1) year unless the Contract has not been terminated by one of the parties at least (3) months before the end of the contract term.

6.2 Furthermore, both the Provider and the Customer shall be able to terminate the contract due to important reasons without notice.

6.3 Notices of termination shall only be valid in written form.

7. Remuneration

7.1 The remuneration for the licensing and use of the cloud service shall be agreed by both parties within the order documents of the Provider.

7.2 The remuneration for the agreed period is due in advance and shall be invoiced to the Customer by the Provider.

8. Usage rights of the cloud service and protection against unauthorized use

8.1 A non-exclusive right to use the cloud service and the documentation by remote access within his own business purposes shall be granted to the Customer during the term of the contract.

8.2 Further use shall be contractually agreed prior to its use. The remuneration shall be based on the scope of the right of use.

8.3 The Provider is entitled to take appropriate technical measures as a protection against use that is not in line with the provisions of the Contract.

8.4 The Provider shall be entitled to revoke the Customer's right of use if the latter significantly contravenes any restrictions on use or any other regulations ensuring protection against unauthorized use (see also Section 1.3 and Section 10.4). Prior to this, the Provider shall set a period of grace for

the Customer to remedy the situation. In case of recurrence and particular circumstances, which justify immediate revocation, after taking both parties mutual interests into consideration, the Provider shall be entitled to revoke the Contract without a period of grace. After the revocation the Customer is obliged to confirm the abandon of use to the provider in written form. The Provider shall grant the right of use to the Customer again after the Customer has assured and explained in writing that infringements against the right of use are no longer present and previous infringements and their consequences have been removed.

9. Engagement of subcontractors

9.1 The Provider shall be entitled to engage subcontractors to fulfil his obligations. The customer already declares its consent to this.

10. Obligations of the Customer

10.1 The Customer shall ensure that professional staff is available for the support of the Provider and the use of the cloud service during the term of Contract.

10.2 The Customer shall provide support to the Provider in remedying deficiencies if necessary. In particular, the Customer is obliged to describe the deficiencies in detail and in written form and provide all relevant data, documents and information if requested by the Provider.

10.3 The Customer shall acknowledge that the cloud service including the operating instructions and all other related documents - including future versions - are copyrighted.

10.4 The Customer shall not carry out any action which could aid unauthorized usage. The Customer is obliged to inform the Provider without delay if he have any reason to suspect unauthorized access.

11. Defect claims of the Customer

11.1 For warranty claims the defect regulating provisions of leasing law shall apply. Cloud service defects shall be remedied by the Provider as described in Section 4. The customer shall not enforce a reduction in payment by deduction from the agreed remuneration. Related claims for enrichment or compensation shall remain unaffected.

11.2 The Customer’s right of termination to the failure to grant use in accordance with the agreement, unless the contractually agreed use is deemed as failure.

11.3 The Provider ensures warranty for the contractually agreed purpose of the provided services. Defects of quality cannot be claimed for insignificant deviation of the contractually agreed services. Claims for

defects shall also be invalid in the case of improper use, defects that are not reproducible or otherwise provable by the customer, or in case of damages arising particular external influences not foreseen in the terms of the contract. This shall also apply in case of subsequent changes or remedial maintenance carried out by the Customer or a third party, unless it does complicate the analysis and the removal of the defect. In addition to this, Section 13 et seq. shall apply to claims for compensation of damages and expenditure.

11.4 The period of limitation for any claims arising from material defect shall be one year. The processing of the customer's report of a defect shall lead only to suspension of the period of limitation, insofar as the legal prerequisites for this exist. The period of limitation shall not recommence as a result of this. A subsequent rectification (new delivery or repair) shall effect exclusively the period of limitation of the defect which led to the subsequent rectification.

11.5 The Provider can insist on remuneration of his effort as (1) he carried out any activities on the basis of a report without a defect existing, unless the customer was unable to recognize with reasonable effort that no defect existed, or (2) a reported defect is not reproducible, or (3) additional expenses accrue due to improper performance of the Customer's obligations (also see Section 10 et seq.).

12. Defects of title

12.1 The Provider shall only be liable for infringements of third party rights through the delivery of its service insofar as the service is used in conformity with the contract and especially in the operating environment described in the contract. The Provider shall only be liable for the infringements of third party rights at the place of contractual use of the service.

12.2 If a third party asserts against the Customer that a service provided by the Provider infringes its rights, the Customer shall inform the Provider without delay. The Provider and, if appropriate, its sub-contractors are entitled but not obliged to defend unjustified claims at their own expense. The Customer shall not be entitled to assert third-party claims before he has appropriately given the Provider the opportunity to repel third-party rights by any other means.

12.3 If third-party rights are infringed by any service, the provider shall proceed as follows at his own choice and costs and (1) shall provide the Customer with the right to use the service, or (2) provide the service without infringing any rights, or (3) if the Provider cannot achieve another remedy given a reasonable amount of effort, the Provider shall withdraw the service and refund the Customer the remuneration paid by it (less an appropriate usage fee). The interests of the Customer shall be appropriately taken into consideration.

12.4 Customer claims due to defects of title expire by limitation in accordance to Section 11.4. Section 13 et seq. shall additionally apply for all Customer claims of damage or compensation. Section 11.5 shall additionally apply for additional effort and expenses of the Provider.

13. General liability of the Provider

13.1 The Provider shall be liable to the Customer (1) for damages he or his legal representatives or assistants have caused either purposely or by culpable negligence, and (2) for damages deriving from the loss of life, bodily injury or harm to health that the Provider, his legal representatives or vicarious agents are responsible for.

13.2 The Provider shall not be liable in the case of slight negligence, unless it has breached an essential contractual obligation, whose fulfilment enables the proper implementation of the contract and whose observance is regularly trusted and should be presumable by the Customer. This liability shall be limited to damages that are foreseeable and typical of the contract, this shall also apply to lost profit and cost savings failing to occur. Liability for other remote subsequent damage is excluded. For a single claim, the liability shall be limited to the contractual value and in the case of current payments to the value for one contractual month. Section 11.4 shall apply to the limitation accordingly. Liability according to Section 13.1 shall remain unaffected by this paragraph.

13.3 The Provider shall only be liable for compensation of damages arising from a warranty if this is expressly adopted in the warranty. In case of slight negligence this liability shall apply according to the limitations of Section 13.2.

13.4 In the case of loss of data, the Provider shall only be liable for the expenditure which is necessary to restore the data in the case of the Customer having made a proper data backup (see Section 14.2).

14. Data protection and copies of Customer data

14.1 As far as the Provider can access data, and especially personal data, that is stored on the Customer's system, he shall only be active as an order data processor and only process and utilize this data for the purpose of Contract fulfilment. The Provider shall follow to the Customer's instructions for handling this data. The Customer shall be liable for any disadvantageous results of such instructions for fulfilment of the Contract.

14.2 The Customer shall download the electronic copy of the Customer data in encrypted form from the Provider once per calendar month, thereby saving it and securely storing it as his own backup.

14.3 At the end of the contractual period of use, the Provider shall provide the backup of the last day of this contractual period of use within 48 hours. The Customer has the right to download this backup,

as stated in Section 14.2, within 10 days. Subsequently, the Provider shall irrevocably delete all data of the Customer.

14.4 The Provider processes data on behalf of the Customer (All common and relevant data that are stored in ERP (especially SAP) and related sub-systems. In particular, this includes the following data: Customers, suppliers and those interested with data concerning contact persons. Personal data (applicants, employees, trainees, interns, retirees, etc.). Data on recording working time, equipment access control and scheduling. Data for communication as well as carrying out and monitoring transactions as well as technical systems, emergency contact data; other groups of individuals.) This includes activities that have been specified in the service description (Operation of SAP and sub-systems Consultation on optimizing and using SAP and sub-systems; Configuration and provision of SAP and sub-systems; Troubleshooting and data correction in SAP and sub-systems; Transfer and processing of data to load in the SAP system and sub-systems. On request of the Customer, processing of data for the transfer to third parties; e.g. personal data to billing systems; electronic transaction forms to banks, data bases to software manufacturers (e.g. SAP) for further error analysis and correction in SAP and sub-systems). Within the scope of this contract, the Customer is solely responsible for complying with the legal regulations of the data protection law, particularly for the lawfulness of passing on data to the Provider as well as for the lawfulness of data processing.

14.5 Initially, the instructions will be defined through the Contract and can afterwards be changed, amended or replaced by individual instructions by the Customer in written form or text form (individual instructions). Instructions that go beyond the service agreed upon within the scope of the Contract shall be treated as a request for a service change.

14.6 The Provider may only process the data of those involved within the scope of the order and the instructions of the Customer.

14.7 Within its sphere of responsibility, the Provider shall design the in-house organization in such a way that it meets special data protection requirements. He shall take technical and organizational measures for the adequate protection of the Customer's data that meet the requirements of the Data Protection Law. These measures concern: (1) Entry control, (2) Admission control, (3) Access control, (4) Transfer control, (5) Input control, (6) Order control, (7) Availability, and (8) Separation. The security measures carried out by the Provider are specified in the following. The Contractor reserves the right to change of the safety measures involved, whereby it must however be ensured that the protection level that has been contractually agreed on is not exceeded.

14.7.1 Entry control

In particular, the Provider shall execute the following measures in order to prevent unauthorised individuals access to data processing systems with which data is processed or utilised (entry control): (1) Introduction and maintenance of graduated access rights for employees and third parties; (2) Regulation and limiting access rights, handing out related keys or key cards; (3) Regular inspection and update of keys or key cards; (4) Identification and validation of all persons with access rights; (5) Keeping a log of visitors that have access to data processing systems

14.7.2 Admission control

In particular, the Provider shall execute the following measures in order to prevent data processing systems to be used by unauthorised individuals (admission control): (1) Operation of central data processing systems (servers) only in specially secured rooms to which only select employees (administrators) and service providers have access that are obligated to diligence and secrecy; (2) Creation and implementation of rules of conduct for the use of mobile terminal equipment that obligates the employees, among other things, not to leave these devices unattended during travel; (3) Logical (e.g. passwords) and physical (e.g lockable or otherwise secured containers) protection of all data storage media (external hard drives, USB sticks, CD-ROMs, DVDs etc.).

14.7.3 Access control

In particular, the Provider shall execute the following measures in order to ensure that those authorised to use a data processing system only have access rights to data regarding their authorization, and that data cannot be read, copied, modified or deleted during processing, usage and after saving (access control): (1) Creation and implementation of usage guidelines regulating the collection, reading, modifying and deletion of data; (2) Usage of the data processing systems only after identification and authentication of the user; (3) Blocking of user accounts provided that these have not been used for a period of longer than 30 days; usage of secure passwords; (4) Regularly changing passwords; (5) Blocking passwords after having entered them incorrectly several times; (6) Limiting of user rights for employees that are not administrators; separation of testing and productive systems.

14.7.4 Transfer control

In particular, the Provider shall execute the following measures in order to ensure that data can't be read, copied, changed or removed without authorization during electronic transfer, transportation or saving on data carriers, and that it can be tracked and verified, at which points a transmission of data by appliances for data transfer is designated (transfer control): (1) Creation and execution of a guideline of use which regulates the transfer and transport of data; (2) Usage of data processing appliances only after identification and authentication by the user; (3) Creation of documentations

for all programs that encrypt, send or receive data; (4) Monitoring of all interfaces (Ports) of the data processing appliance to the internet, and blocking of all interfaces usually not needed (e.g. ports which are used for file-sharing applications or chat applications); (5) Monitoring of local company sites, insofar as those send or receive data.

14.7.5 Input control

In particular, the Provider shall execute the following measures in order to ensure that it can retroactively be tracked and verified, if and by whom data has been entered in, changed or removed from data processing systems (input control): (1) Creation and execution of a guideline which regulates the recording, reading, changing and removing of data; (2) Usage of the data processing appliance only after identification and authentication of the user; (3) logging of relevant accesses to data.

14.7.6 Order control

In particular, the Provider shall execute the following measures in order to ensure that data, which is processed by order, will only be processed according to the instruction of the Customer (order control): (1) Usage of the data processing appliance only after identification and authentication by the user; logging of relevant access to data.

14.7.7 Availability

In particular, the Provider shall execute the following measures in order to ensure that data is protected against coincidental destruction or loss (availability): (1) Creation of backups at least once within 24 hours on two different systems minimum; (2) Storage of backups in flame-proofed containers or a data centre separated by open ground.

14.7.8 Separation

In particular, the Provider shall execute the following measures in order to ensure that various data, which has been gathered for different purposes, will be processed separately (separation): Logistical separation of the data from the customer and other data.

14.8 The Provider shall ensure that it is mandatorily forbidden for the employees and other persons, who are active in the processing of the Customer's data, to collect, process or utilise data in an unauthorised manner. Data secrecy shall remain in effect even after completing the order.

14.9 The Provider shall inform the Customer about severe infringements by the Provider without any delay, as well if persons hired by the Provider within the scope of the order infringe upon the regulations to protect the data of the Customer or the determinations of the present Contract. He

shall take required measures to secure data and to reduce possibly adverse consequences to those involved and shall immediately seek agreement with the Customer regarding the matter. The Provider shall provide support to the Customer to meet the information requirements.

14.10 The Provider shall appoint a contact person for the Customer regarding data protection issues within the scope of the present Contract.

14.11 The Provider shall not use the provided data for any other purposes than for fulfilment of the Contract.

14.12 The Provider shall correct, delete or block the data specified in the present Contract if the Customer instructs to do so. The Provider assumes the data-protection-conform destruction of data carriers and other materials due to an individual order by the Customer, provided that it has not already been arranged in the Contract. In special, by the Customer to be defined cases, a storage and handover will be carried out.

14.13 Data, data carriers as well as all other materials must be handed over or deleted after the end of the order by request of the Customer.

14.14 In the case of test and scrap material, an individual order is not required.

14.15 If additional costs accrue due to deviating requirements when handing over or deleting the data, these shall be carried by the Customer.

14.16 The Customer must immediately and fully inform the Provider if he determines errors or irregularities regarding data-protection-related regulations in the order results.

14.17 It is the Customer's obligation to manage the public procedure index.

14.18 If, on account of applicable data protection laws, the Customer is obligated toward an individual to provide information on the collection, processing or utilisation of data of this person, the Provider shall thereby provide the Customer with support to make this information available. This assumes that the Customer has made a request in written or text form and the Customer reimburses the Provider the costs that have arisen due to this support. The Provider shall not answer any requests for information and, in this respect, shall refer the affected person to the Customer.

14.19 If an affected person addresses the Provider with demands to correction, deletion or blocking, the Provider will refer the affected person to the Customer.

14.20 Before starting data processing activities, the Customer shall convince himself of the technical and organisational measures of the Provider, continue this on a regular basis, and shall document the results. For this purpose, he can, for example, obtain the Provider's information, have an existing certificate, if available, presented that has been issued by an expert, or, following timely coordination, perform an inspection during normal business hours without disturbing operations, or have an inspection performed by an expert third party, provided that the third party is not in direct competition with the Provider.

14.21 The Provider shall tolerate the inspections of the Customer and, on written request, shall undertake to provide the Customer all information and certificates that are required to carry out an inspection within a reasonable time. The Customer shall reimburse the cost and expenses to the Provider that accrue due to the Customer's inspections.

14.22 The Customer shall agree that the Provider may seek the assistance of associated companies of the Provider in order to fulfil the services agreed upon within the present Contract, or sub-contract companies with the specified services.

14.23 The contractually agreed services and the partial services listed in the following shall be carried out by involving one sub-contractor in particular, namely SAP AG, Walldorf (Germany), for the provision and maintenance of the SAP software

14.24 If the Provider issues orders to a sub-contractor, the Provider shall undertake to transfer its obligations deriving from the present Contract to the sub-contractor. Sentence 1 shall particularly apply to requirements concerning confidentiality, data protection and data security between the contractual parties of the present Contract. A possible inspection on behalf of the Customer at the sub-contractor's place of business shall only take place in coordination with the Provider.

14.25 Upon written request, the Customer shall be entitled to receive information from the Provider on data-protection-relevant obligations of the sub-contractor as well as insight into relevant contractual documents if required.

14.26 A sub-contracting relationship subject to approval shall not be deemed valid if the Provider commissions a third party within the scope of a supplementary service to the primary service, such as in the case of external personnel, postal and shipping services or maintenance.

14.27 The Provider shall make agreements with this third party at the scope required in order to ensure adequate data protection.

14.28 In case the data of the Customer become endangered in the possession of the Provider due to seizure or confiscation, insolvency or settlement proceedings, or because of other events or measures taken by third parties, the Provider must inform the Customer about this immediately. The Provider shall immediately inform all those responsible in this respect that the sovereignty and ownership of the data exclusively lies within the scope of the Customer as a responsible authority.

15. Rights of SAP

15.1 The Customer shall make notice that the Provider must regularly present to SAP reports about his customers – this also includes the Customer. For this purpose, the Customer shall agree that the Provider will transmit the following information to SAP: (1) SAP order number for the Customer; (2) Name of the Customer; (3) Customer address (street, postal code, city, country); (4) DUNS number of the Customer (Dun & Bradstreet's number for the purpose of clear identification of the company); (5) Status of the Customer (basic terms of the Contract/cancellation deadline, number and type of the Customer's users); and (6) other details regarding the Customer as requested from the Provider by SAP in accordance with their contractual agreement.

15.2 The Customer shall treat the sensitive information from SAP at least as confidentially as the information of the Provider in accordance with Section 16 et seq., and ensure that its defined users do the same.

15.3 The Customer shall grant SAP the right (as a true right to the benefit of third parties) to assert damage compensation claims in the case of the Customer's infringement upon the rights of SAP regarding intellectual property.

15.4 Furthermore, the Customer is obliged to ensure that SAP can carry out tests – in accordance with applicable data protection laws –, in order to (1) comply with licencing provisions for SAP software, (2) calculate fees between the Provider and SAP, and/or (3) verifiy the accuracy and completeness of the reports made by the Provider to SAP, and to obtain the required consent for receiving such verifications of individuals that work for the Customer.

15.5 Subject to legal limitations, and without collecting content or other confidential information and transferring this to SAP, SAP shall be permitted, (1) to set up the SAP software in such a way that each system generates the required information for an inspection, thereby transferring it to SAP, and (2) to remotely access the SAP software and the equipment it is installed on to examine its use.

16. Confidentiality

16.1 Each party shall treat as confidential all sensitive information, protected information, and business secrets of the other party that may be obtained in connection with the present Contract. Each party

shall treat this Contract and its terms as confidential information. The parties shall provide their employees or third parties with confidential information only as far as this is required to fulfil their obligations within the scope of the present Contract and only under the conditions that these individuals are subject to a corresponding duty of professional secrecy.

16.2 Confidential information does not include any information that: (1), without fault of the receiving party, are generally known or publicly accessible; (2) was in the possession of the recipient party without infringing upon an obligation to secrecy before receiving it from the disclosing party, or the information was known or acquired in physical form; (3) was independently developed by the recipient party without using the confidential information; (4) was properly disclosed to the recipient party by third parties who are not subject to any secrecy obligation with reference to the information; (5) was disclosed by the recipient party having received previous written consent from the disclosing party; (6) according to legal or regulatory provisions, must be disclosed if the disclosing party is informed without undue delay of this obligation and the extent of the disclosure shall be limited to the furthest extent possible or information that must be disclosed due to a court ruling if the disclosing party is informed of this ruling without undue delay and there is no possibility to make an appeal against the ruling.

16.3 The aforementioned confidentiality obligations shall continue even after ending this Contract.

17. Miscellaneous

17.1 The Customer shall respect self-dependently the applicable import and export regulations for the services. In case of transboundary services, the Customer shall be responsible for incurring customs, fees and other dues. The Customer shall process self-dependently legal or governmental procedures concerning transboundary services, except when otherwise and explicitly agreed.

17.2 German law applies. The application of the United Nations Convention on Contracts for the International Sale of Goods (CISG) is not permitted.

17.3 The acceptance of services by the Customer applies as acknowledgement for the general conditions of contract by the Provider. Other conditions are only binding if the Provider acknowledged them in writing.

17.4 Changes and amendments of this contract shall be made in written form.

17.5 The place of jurisdiction is the domicile of the Provider. The Provider can also sue the Customer in whose domicile.