Agreement on the Cloud-Based Use of Software ("Software as a Service")

between

ASMPT GmbH & Co. KG
Rupert-Mayer-Str. 48
81379 Munich, Germany

- hereinafter referred to as "**ASMPT**" and/or "Processor"-

and

Contractual partner

- hereinafter referred to as the "**Customer**" and/or "Controller"-

hereinafter referred to collectively as the "**PARTIES**" and individually as the "**PARTY**".

Preamble

This agreement on the cloud-based use of software ("Software as a Service") – "**AGREEMENT**" – is concluded between ASMPT and the CUSTOMER. The term CUSTOMER as it is used in this agreement refers to the CUSTOMER and the affiliated companies of the CUSTOMER as defined in §§ 15 et seq. of the German Stock Corporation Act (AktG)("**AFFILIATED COMPANIES**") unless the context suggests otherwise.

ASMPT shall render services to the CUSTOMER by providing access to its own cloud-based software, which is described in **Annex 1** (Specification of Services) ("**SOFTWARE**"). The hardware and software environment (Infrastructure as a Service, Platform as a Service and Software as a Service including Kubernetes functionalities) which can be accessed via the cloud is provided by a third party to host the software licences of the CUSTOMER and its data ("**CLOUDSTRUCTURE AS A SERVICE**" or "**CAAS**"). ASMPT shall make these contractual services available to the CUSTOMER as a subscription service via a SUBSCRIPTION licence. "**SUBSCRIPTION**" means that the use of the SOFTWARE is limited to a time frame agreed mutually in this AGREEMENT between ASMPT and the CUSTOMER. A SUBSCRIPTION licence can be extended mutually between the PARTIES for one or more limited time periods after the initial term of the SUBSCRIPTION license has expired. However, a SUBSCRIPTION licence cannot be converted into an unlimited licence. Maintenance services for the SOFTWARE and further developments of the SOFTWARE are included in the SUBSCRIPTION licence fees. In the case of multi-year SUBSCRIPTION licences, ASMPT reserves the right to demand that new licence keys are used periodically during the term of the SUBSCRIPTION licence. ASMPT reserves the right to exclude certain versions of its software products and/or third-party products sold by ASMPT from a SUBSCRIPTION licence.

This agreement shall form the basis for the cloud-based use of the SOFTWARE by the CUSTOMER and its AFFILIATED ENTERPRISES. The cloud solution shall be provided as CLOUDSTRUCTURE AS A SERVICE by a third party with whom ASMPT has concluded an appropriate contractual agreement.

All terms written in upper case in this AGREEMENT bear the meaning stipulated in this AGREEMENT.

In light of the above, the PARTIES agree the following:

§ 1 Subject of the AGREEMENT, Scope of the Services

1. The subject of the AGREEMENT is the licencing of the SOFTWARE as a cloud solution which is described in detail in **Annex 1** (Specification of Services) and the licensing of the usage rights described in § 4 for a limited period of time (term of the SUBSCRIPTION). The PARTIES have not agreed any additional services in addition to the services defined explicitly in the AGREEMENT. ASMPT shall provide the CUSTOMER with the SOFTWARE described in **Annex 1** (Specification of Services) by means of an Internet-based cloud solution provided by a third party as CAAS for the term of the SUBSCRIPTION for its own use ("Software as a Service"). This will enable the CUSTOMER to save and process data on the storage space provided by the third party as CAAS during the term of the SUBSCRIPTION. The scope of use of the software and storage space is also described in the specification of services in **Annex 1** (Specification of Services). The scope of use shall not include the provision of the software for installation on the CUSTOMER's systems.

2. ASMPT shall be entitled to sub-contract third parties for the provision of the services, and particularly to make use of third-party cloud services as CAAS.

3. For the cloud-based services made available by ASMPT, ASMPT ensures an availability of at least 98.5% per year. This availability relates to the total annual time of one calendar year. The decisive factor is the availability of the SOFTWARE at the transfer point of the SOFTWARE to the Internet. Downtime shall not include any time when the SOFTWARE cannot be used as a result of technical or non-technical issues caused by the CUSTOMER, nor shall it include any time during failures over which ASMPT has no control (e.g. external DNS faults, attacks on network and mail systems, failures of parts of the Internet, force majeure, third-party fault), or any time during scheduled maintenance work announced to the CUSTOMER in advance. The conditions stipulated in **Annex 2** (CLOUDSTRUCTURE AS A SERVICE Conditions of the Third Party) shall apply to the cloud provided within the framework of this AGREEMENT by the third party as CLOUDSTRUCTURE AS A SERVICE, unless otherwise explicitly stipulated in this AGREEMENT.

4. ASMPT's performance obligations and therefore also this agreement do not cover the CUSTOMER's connection to the Internet, the maintenance of its network connection, or the quality and provision of any hardware and software required by the CUSTOMER.

5. ASMPT shall provide the CUSTOMER with the login details needed to use the software in such a form and to such an extent that all authorised users of the CUSTOMER can access the software in accordance with their authorisation concept.

6. The licence of the SOFTWARE for the CUSTOMER and its use by the CUSTOMER are subject solely to this AGREEMENT. ASMPT does not recognise General Terms and Conditions of Business of the

CUSTOMER which contradict this AGREEMENT, deviate from legal provisions or change this AGREEMENT unless ASMPT has explicitly agreed to their validity. This consent requirement also applies in all cases where ASMPT in knowledge of the General Terms and Conditions of Business of the CUSTOMER provides the service unconditionally or accepts payments in knowledge of the General Terms and Conditions of Business of the CUSTOMER.

7. By accessing the SOFTWARE as CUSTOMER or by using the SOFTWARE or registering for it, the CUSTOMER agrees with the following:

(a) this AGREEMENT

(b) **Annex 1** (**Specification of Services**)

(c) **Annex 2** (**CLOUDSTRUCTURE AS A SERVICE Conditions of the Third Party**)

(d) **Annex 3** (**Privacy Statement of ASMPT)** - " **Privacy Statement**" -,

(e) if necessary, the ASMPT agreement on data processing ("**DATA PROCESSING AGREEMENT**") which is attached to this AGREEMENT as **Annex 4**.

8. The AGREEMENT and its annexes regulate the use of the SOFTWARE by the CUSTOMER and the access of the CUSTOMER to the SOFTWARE in the cloud.

9. The CUSTOMER must be registered and logged in to be able to use the SOFTWARE.

10. After the login data has been provided, the SOFTWARE shall be provided to the CUSTOMER as a cloud solution for the term of the SUBSCRIPTION so that the CUSTOMER can use and apply the SOFTWARE within the framework of the usage rights granted.

11. The CUSTOMER's obligations to cooperate described in § 2 are not part of ASMPT's performance obligations. ASMPT is therefore not responsible for the CUSTOMER's Internet connection to the SOFTWARE and any Internet, hardware, software, technical and licencing requirements to be fulfilled by the CUSTOMER.

12. All statements and declarations made by ASMPT regarding the SOFTWARE which are made in advertising materials, on websites and in the documentation with the exception of the specification contained in the AGREEMENT are only a description of the design and are not to be understood as a guarantee or contractual warranty of a property.

13. ASMPT reserves the right to modify the SOFTWARE, to further develop the SOFTWARE, to adapt it to the state of the art or to optimise it, in particular to improve its user-friendliness. A prerequisite for such a change is that it is necessary to fix bugs, correct errors, update and complete the SOFTWARE, optimize the program or adapt it for licensing reasons. If such a modification results in a serious impairment to the services to which the CUSTOMER is entitled and if ASMPT, despite a written request from the CUSTOMER, does not remove the impairment by providing a solution that meets the needs of the CUSTOMER in the same way as before the modification or adaptation, the CUSTOMER is entitled to demand either a reduction in the remuneration commensurate with the impairment or to terminate the AGREEMENT without notice, if ASMPT does not correct at least 90% of the impairments reported by the CUSTOMER per calendar year within 30 calendar days.

§ 2 Obligations to Cooperate

1. Unless explicitly agreed otherwise in writing, or unless indicated otherwise in **Annex 1** (Specification of Services), the CUSTOMER may access the cloud from any computer or any mobile device that provides access to the internet for the term of the SUBSCRIPTION.

2. The contractually agreed use of ASMPT's services shall be dependent on the fact that the hardware and software used by the CUSTOMER – including any workstations, routers and data communication equipment etc. – meets the technical requirements and the users authorised by the CUSTOMER to use the software are familiar with its operation. The CUSTOMER shall guarantee to keep its communication devices in good working order during the term of the SUBSCRIPTION and to maintain their functional capability in accordance with the respective applicable state of the art. The CUSTOMER shall undertake to ensure that the requirements defined in **Annex 1** (Specification of Services) are adhered to. If the CUSTOMER does not fulfil this obligation for reasons for which it is itself responsible, ASMPT is not responsible for any resulting functional limitations.

3. The CUSTOMER may only use the services to the extent necessary within its ordinary course of business. The CUSTOMER shall avoid the excessive use of the services and capacities so as not to impair the provision of the services to all of ASMPT's users and to ensure the security of the network.

4. If the CUSTOMER jeopardises the security, integrity or availability of ASMPT's networks, servers, SOFTWARE or data through its use of the services, or if ASMPT has an objective reason to suspect the potentially serious disruption of its networks, SOFTWARE or saved data, ASMPT may temporarily or permanently remove or restrict the CUSTOMER's access to the services. Any time that passes with removed or restricted access shall not be considered when calculating downtime.

5. The access of the AUTHORISED USERS of the CUSTOMER to the SOFTWARE requires the registered user names of the AUTHORISED USERS of the CUSTOMER to be provided; such access is protected by a password and is granted with this login data, which allows the AUTHORISED USERS of the CUSTOMER to log in. The CUSTOMER must maintain strict secrecy with regards to any passwords received from ASMPT or sent by ASMPT provided SOFTWARE for the purpose of accessing the services, and to prevent unauthorised third-party use, and the CUSTOMER must notify ASMPT immediately if it discovers that a password has become known to unauthorised third parties. In the event of misuse, ASMPT is entitled to remove access to the SOFTWARE until the circumstances are clarified and the misuse has stopped. The CUSTOMER is liable for any misuse occurring in its sphere of responsibility. The CUSTOMER shall oblige its AUTHORISED USERS accordingly in writing on behalf of ASMPT before the respective AUTHORISED USERS access the SOFTWARE for the first time. "**AUTHORISED USERS**" means (i) the employees of the CUSTOMER and (ii) the employees of the AFFILIATED COMPANIES and if necessary external companies of the CUSTOMER. The CUSTOMER shall undertake to prevent unauthorised third-party access to the SOFTWARE and the documentation of this by taking suitable precautionary measures within the bounds of what can reasonably be expected of it. The AUTHORISED USERS of the CUSTOMER must be made firmly aware of the mandatory need to adhere to the preceding contractual provisions and the provisions of copyright law.

6. The CUSTOMER shall bear its own costs which arise for the use of the SOFTWARE such as for separate Internet access or for the corresponding hardware and software, for example.

7. If the SOFTWARE is developed further, the CUSTOMER is obliged, after being appropriately informed by ASMPT, to make the necessary modifications to its IT infrastructure.

8. The CUSTOMER must take the necessary measures to secure his systems, in particular to to keep his system up to date (e.g. operating system, applications, browser, virus scanner, …), to use the latest security settings to protect the system with a firewall and to use the latest protection mechanisms to defend against malware.

9. The CUSTOMER's obligations to cooperate described above are a compulsory prerequisite for the provision of the contractual services by ASM; they must be performed by the CUSTOMER at the latest when the contract is concluded and must be upheld for the entire term of the contract.

§ 3 Technical Support via Phone and Email

1. ASMPT shall provide support within the framework of the contractual AGREEMENT during the term of the SUBSCRIPTION in accordance with **Annex 1** (Specification of Services).

2. ASMPT shall set up a special hotline for this purpose to be reached via phone and email during ASMPT's business hours (see **Annex 1** for details) during the term of the subscription. The provision of a telephone hotline outside business hours shall be the subject of an explicit agreement.

3. The hotline shall include an information service for the SOFTWARE used; it shall be granted for a typical amount of questions related specifically to the programme.

§ 4 Intellectual property rights, usage rights to the SOFTWARE

1. ASMPT remains the owner of all rights to the SOFTWARE, even if the CUSTOMER modifies the SOFTWARE or connects it to its own programs or contents or those of a third party. The CUSTOMER is the owner of all results and contents which it has generated in or with the SOFTWARE.

2. The computer programs, in particular the SOFTWARE, are protected in accordance with §§ 69a et seq. of the German Copyright Act (UrhG). Any third-party rights to the protected work remain unaffected.

3. Trademarks, logos, other symbols or protection notices, copyright notices, serial numbers and other identification features may not be removed or changed either in electronic format or in printouts.

4. ASMPT shall grant the CUSTOMER and its AFFILIATED COMPANIES a non-exclusive, non-transferrable and non-sublicensable right, limited to the term of the SUBSCRIPTION, to use the SOFTWARE including all updates and upgrades which ASMPT provides to the CUSTOMER for the term of the SUBSCRIPTION by way of a "Software as a Service" cloud-based solution. In terms of content, the usage right is restricted to the permitted use provided for in this AGREEMENT for the term of the SUBSCRIPTION. Permitted use encompasses loading the SOFTWARE into the main memory and running the SOFTWARE as well as its proper use by the CUSTOMER. The CUSTOMER may only copy the SOFTWARE to the extent that its respective installation and reproduction are necessary for it to be used. Otherwise, the type and scope of the use is defined in **Annex 1** (Specification of Services). The CUSTOMER shall be granted no further rights to the SOFTWARE or any other industrial property rights

associated with the Specification of Services. Downloaded documents may generally only be saved for the duration of the SUBSCRIPTION term.

5. The CUSTOMER shall not be entitled to use the SOFTWARE beyond the permitted use specified in the Specification of Services, nor may it allow the software to be used by third parties or otherwise make it accessible to third parties. In particular, the CUSTOMER shall not be permitted to reproduce, reverse engineer, decompile or disassemble any part of the software, unless this is explicitly permitted. In derogation of the restrictions defined above in § 4 (5), the CUSTOMER is authorised to decompile the SOFTWARE provided that this is necessary to ensure the interoperability of the SOFTWARE with other programs. However, the prerequisite for this is that ASMPT has not provided the CUSTOMER with the required information upon request within an appropriate period of time.

6. The SOFTWARE may contain third-party technology, including open-source software, which is supplied with the SOFTWARE, or make the use of such technology necessary. For third-party technology, the CUSTOMER is given a licence either in accordance with the conditions of this AGREEMENT or in accordance with separate licencing conditions which are defined in the relevant documentation, "Readme" files, license files, note files or other such documents or files (**"TECHNOLOGY SUBJECT TO THIRD-PARTY LICENCES"**). The rights of the CUSTOMER to use TECHNOLOGY SUBJECT TO THIRD-PARTY LICENCES are subject to these separate licencing conditions and are in no way restricted by this AGREEMENT. Provisions of this AGREEMENT which contradict a mandatory applicable law accorded by a third-party licence shall not apply. If an applicable third-party licence requires ASMPT to provide a source code contained in the TECHNOLOGY SUBJECT TO THIRD-PARTY LICENCES, ASMPT shall provide this upon written request, if necessary, in return for payment of the costs for shipping and handling. To clarify: third-party technology which is not TECHNOLOGY SUBJECT TO THIRD-PARTY LICENCES is regarded as part of the SOFTWARE for which the CUSTOMER is granted a licence in accordance with the conditions of this AGREEMENT.

7. ASMPT is entitled to take technical measures to prevent use that goes beyond the permitted scope, in particular by installing an appropriate program for blocking access. The CUSTOMER may not use any devices, products or other means which serve to avoid or transcend the technical measures taken by ASM. In the event of misuse, ASMPT is entitled to block access to the SOFTWARE immediately. Further rights and claims of ASMPT, in particular the right to terminate the contract without notice for good cause as well as claims for damages shall remain unaffected.

8. The CUSTOMER must immediately provide ASMPT with any information it requests to assert claims against third parties following their unauthorised use of the software.

9. The CUSTOMER is liable for all damages and payments which arise directly from the unauthorised use of the services of ASMPT by third parties if the unauthorised use can be attributed to a wilful act or omission of the CUSTOMER or its AUTHORISED USERS.

§ 5 Use of storage space ("web hosting") in the cloud

1. ASMPT shall provide the CUSTOMER with a necessary amount of storage space via a third-party provider as CAAS.

2. The use of storage space provided via the cloud may only occur within the framework of using the SOFTWARE. In particular, the CUSTOMER shall only be authorised to upload and download data if this is explicitly envisaged within the contractual use of the SOFTWARE.

3. The conditions stipulated in **Annex 2 (CLOUDSTRUCTURE AS A SERVICE Conditions of the Third Party)** shall apply to the cloud provided within the framework of this AGREEMENT by the third party as CLOUDSTRUCTURE AS A SERVICE, unless otherwise explicitly stipulated in this AGREEMENT.

§ 6 Warranty

1. ASMPT shall guarantee that it holds all the necessary rights to grant the CUSTOMER the rights and licences to be granted under this AGREEMENT.

2. ASMPT shall not assume a warranty for any defects caused by the CUSTOMER's failure to follow the operating or maintenance instructions when operating the hardware and SOFTWARE, nor shall it assume a warranty for any defects caused by changes made by the CUSTOMER.

3. Minor deviations from the contractually agreed quality and/or performance of the services shall not constitute defects.

4. The CUSTOMER is responsible for preventing security problems in relation to its own systems and data, including the SOFTWARE hosted on the CUSTOMER's systems. The CUSTOMER's responsibility encompasses but is, however, not limited to undesired intruders in the SOFTWARE such as malware, viruses, spyware or trojans, and ASMPT disclaims all responsibility for damages which arise as the result of the failure of the CUSTOMER to back up its systems and data as well as keep them up to date.

5. For the term of the SUBSCRIPTION, ASMPT shall licence SOFTWARE which is free of material and legal defects to the CUSTOMER. Defects which only result in an insignificant reduction in the usability of the SOFTWARE shall not be taken account of. Impairments of use which result from the sphere of the CUSTOMER or the browser or the Internet access provider (such as e. g. hardware, operating errors, faults in computer networks, data connection, Internet, Force Majeure or other reasons originating from the risk area of the CUSTOMER) in particular are not deemed to be defects.

6. At least 90 % of material and legal defects of the SOFTWARE arising during the term of the SUBSCRIPTION of the AGREEMENT per calendar year shall be rectified by ASMPT within 30 days. ASMPT is not obliged to adapt the SOFTWARE to changed operational conditions and technical and functional developments such as e. g. changes to the IT infrastructure, in particular changes to the hardware or the operating system, changes to the functional scope of competitor products or as the result of establishing compatibility with new data formats.

7. Immediately upon receipt, the CUSTOMER must examine the SOFTWARE for obvious defects and inform ASMPT immediately of their presence unless ASMPT has not disclosed the defect. In the case of all defects arising at a later date, the CUSTOMER shall notify ASMPT within two (2) working days of their discovery. For the purpose of rectifying the defects, the CUSTOMER must provide ASMPT immediately upon request with all information required to rectify the defect.

8. ASMPT accepts no warranty for the licenced SOFTWARE to comply with the particular requirements of the CUSTOMER. The same applies to error states which arise as the result of operating errors of the CUSTOMER or third-party hardware or software or other third-party involvement, e. g. as the result of damage caused by imported malware.

§ 7 Liability

1. Unless this AGREEMENT specifies otherwise, ASMPT shall be liable as follows:

2. ASMPT is liable without limitation for personal injury it is itself responsible for and in the event of material damage for which it is responsible shall reimburse the cost of repairing the damaged items up to a maximum amount of the contractual value of the AGREEMENT.

2. Further claims for damages and reimbursement of expenses, irrespective of the legal reason, in particular due to the infringement of contractual obligations and from unlawful acts are excluded. This in particular concerns claims arising from consequential damages (including consequential damages from defects) such as e.g. lost profit, business interruption, lost usage, interest losses, losses of information and data or third-party contractual claims.

3. The general, strict liability of ASMPT for defects existing at the time the contract was concluded in accordance with § 536a Para. 1 Clause 1 of the German Civil Code (BGB) is excluded.

4. Exclusion and restriction of liability do not apply if there is mandatory liability, e.g. in accordance with the Product Liability Law, in cases of wilful intent, gross negligence, due to injury to life, body or health, the assumption of warranty for the condition of an item, the fraudulent concealment of a defect or the infringement of key contractual obligations. Key contractual obligations are those contractual obligations the fulfilment of which is a prerequisite for enabling the proper fulfilment of the contract in the first place and on whose adherence the CUSTOMER regularly relies and is entitled to rely. Claims for damages for infringing key contractual obligations are however restricted to the typical damage foreseeable for this type of contract, provided that there is no evidence of wilful intent or gross negligence or if ASMPT is liable due to injury to life, body or health.

5. Provided it is legally permissible, the limitation period for claims for damages against ASMPT is one (1) year unless the damage was caused intentionally. In the case of claims for damages in accordance with the Product Liability Law, the statutory statutes of limitations shall apply.

6. Any damage caused by a data leak shall be governed by the liability provisions of the GDPR.

7. The above-mentioned liability regulations do not involve a change to the burden of proof to the detriment of the CUSTOMER.

8. If the liability of ASMPT is excluded or restricted, this also applies to its bodies, employees and vicarious agents.

9. The CUSTOMER is obliged to inform ASMPT immediately in writing of any damage in accordance with the above-mentioned liability provisions or to arrange to have ASMPT record such damage so that ASMPT is informed as early as possible and can minimise the damage in conjunction with the CUSTOMER.

10. Neither PARTY shall be held liable for any delays or unfulfilled contractual duties resulting from events or circumstances beyond their reasonable control (e.g. strikes, lockouts, mistakes by suppliers or subcontractors, pandemics, epidemics, official orders, force majeure or other forms of third-party fault). Any such delays or non-fulfilment shall not be considered a breach of this AGREEMENT, and the contractual term shall be extended for a period matching the duration of the event or circumstances.

11. If the CUSTOMER commits or permits copyright infringements or other legal violations to the detriment of third parties during its use of the SOFTWARE, the CUSTOMER shall be fully liable to ASMPT for any claims asserted by third parties. The CUSTOMER shall indemnify ASMPT against any claims asserted by third parties on basis of such legal violations at the latter's first request. The CUSTOMER shall provide ASMPT with the necessary support in its legal defence and shall also bear any relevant costs incurred by ASM.

12. If the CUSTOMER is accused of infringing third-party rights through the exploitation of intellectual and industrial property rights, it must immediately inform ASMPT of any such allegations. The CUSTOMER must defend itself against such allegations. ASMPT shall be entitled – but not obliged – to participate in such infringement proceedings. Each PARTY shall bear their own costs and any damages owed to third parties.

13. ASMPT shall not be held liable for any data or content transmitted by the CUSTOMER – neither for its correctness, topicality, or completeness, nor for the fact that the data is unencumbered by third-party rights or that the CUSTOMER acts lawfully by processing the data and content using ASMPT's SOFTWARE.

§ 8 Confidentiality and Secrecy

1. The PARTIES agree to maintain secrecy with regard to any confidential information made available to them by the other PARTY during the execution of this AGREEMENT and to only use such information for the fulfilment of the agreement. Furthermore, if one PARTY receives confidential information from the other PARTY, it must take all necessary and reasonable measures to protect the disclosing PARTY's confidential information against unauthorised disclosure or loss.

2. The term "confidential information" is used here to refer to any information which is marked as "confidential", which might be identified as confidential due to its content or the circumstances of its disclosure, or which is of a confidential nature, and which is disclosed or otherwise becomes known to the recipient in a verbal, written, electronic or other form.

3. The term "confidential information" does not apply to any information which:

- is already public knowledge at the time of its disclosure or subsequently becomes accessible to the public without violating this AGREEMENT;
- is already held by the recipient at the time of its disclosure;

- is disclosed to the recipient by a third party without any obligation to maintain confidentiality;
- is developed independently by the recipient without violating this AGREEMENT;
- is not subject to non-disclosure agreements by virtue of the prior written consent of the disclosing PARTY.

4. It shall be incumbent upon the recipient to prove the existence of such exceptional circumstances.

5. The obligation to maintain the secrecy of confidential information shall outlast the duration of this AGREEMENT; it shall continue to apply until the confidential information becomes known to the public.

§ 9 Duration

1. This AGREEMENT is valid starting on the effective date.

2. The minimum term of this AGREEMENT is one year and always ends on the last day of the last calendar month of the minimum term. The basic term or each extension term is not automatically extended. After receiving a notice to prolong the agreement, the customer can extend the duration via a new order.

3. This shall have no bearing on the PARTIES' right to terminate this agreement without notice for good reason. ASMPT shall have a particularly good reason for termination if the CUSTOMER commits a significant breach of its duties stipulated in this AGREEMENT despite receiving prior warning.

4. Upon termination of the AGREEMENT, ASMPT is entitled to block access to the SOFTWARE adhering to a discontinuation right specified in **Annex 1** (Specification of Services) and/or to stop the services. When the AGREEMENT ends, the usage right to the SOFTWARE granted to the CUSTOMER in this AGREEMENT ends.

§ 10 Remuneration

1. The amount of remuneration is detailed in the specific order confirmation.

2. The agreed SUBSCRIPTION fees are due for payment in advance at the beginning of the services month after invoicing with the payment conditions shown in **Annex 1** (Specification of Services) or according to a separate order confirmation. If the services begin during a calendar month, the CUSTOMER will not be billed by ASMPT for this pro rata first month.

3. The CUSTOMER shall only be entitled to offset payments against claims that have been recognised by ASMPT or established by a court of law.

§ 11 Data Protection Provisions

1. The PARTIES agree to comply with the applicable data protection regulations.

2. The CUSTOMER shall in particular warrant that it has obtained all the necessary consents and approvals in accordance with applicable law regarding personal data which the CUSTOMER transfers to ASMPT or provides to ASMPT for processing as part of the software provided for use by means of an Internet-based cloud solution in accordance with this AGREEMENT. The CUSTOMER will compensate ASMPT with regards to all costs, claims, liability, and debts, which accrue for ASMPT in relation to an infringement of this warranty.

3. If ASMPT can access personal data of the CUSTOMER or personal data of natural persons from the sphere of the CUSTOMER, ASMPT will operate exclusively as a processor and will only process and use the above-mentioned personal data to implement this AGREEMENT. If personal data is to be processed and used, ASMPT shall provide the services as part of this AGREEMENT by means therefore of a data processing agreement concluded in accordance with Art. 28 of the General Data Protection Regulation (GDPR). The data processing agreement concluded for this purpose (see **Annex 4**) forms an integral part of this agreement.

4. The CUSTOMER remains the person responsible, both in terms of data protection law and generally in the contractual relationship.

5. The following applies to the internal relationship between ASMPT and the CUSTOMER: in respect of the data subject, the CUSTOMER bears the responsibility for processing and using personal data, provided that ASMPT is not responsible for any claims enforced by the data subject. The CUSTOMER shall review, process and respond to any applications, claims and enquiries of the data subject responsibly. This also applies if a claim is made directly on ASMPT by the data subject. ASMPT shall support the CUSTOMER within the framework of its obligations.

6. ASMPT shall refrain from making any copies or records of the data provided to it and from disclosing such data to third parties – except for any copies and records that are absolutely necessary to ensure proper data processing.

§ 12 Final Provisions

1. This AGREEMENT shall be subject to the substantive law of the Federal Republic of Germany and is to be interpreted accordingly. Regulations on the choice of law which may make the application of the laws of another legal system necessary will not become effective as a result. The United Nations' Convention on the International Sale of Goods (United Nations Convention on Contracts for the International Sale of Goods), whose application is expressly excluded, does not apply to legal transactions within the framework of this AGREEMENT.

2. The sole place of jurisdiction for all disputes arising from or in connection with the contractual relationship is Munich, Germany.

3. Any amendments to this AGREEMENT must be made in writing and signed by the PARTIES. This also applies to any departures from this clause.

4. If individual provisions in this agreement prove to be ineffective or unenforceable, this shall have no bearing on the validity of the agreement as a whole. The PARTIES agree to replace any ineffective or unenforceable provisions with an effective or enforceable clause that best reflects the original economic purpose of the replaced provision. The same applies to any loopholes found in this agreement.

5. This AGREEMENT also extends to the legal successors, legal representatives and permitted assignees of the PARTIES and is binding for them. If this does not happen by operation of law, the PARTIES shall ensure this extension. However, the CUSTOMER may not assign this AGREEMENT and the licences granted within its framework without the prior written agreement of ASMPT, issue sub-licences for it or otherwise transfer it. § 354 a of the German Commercial Code (HGB) (Assignment of Monetary Claims) remains unaffected.

Annex 1

Specification of Services

Software Product:

Virtual Assist – Software as a Service

Specification

Subscription fees apply according to the number and type of packages subscribed to as in the SAP order.

Pricing of the packages will be applied and invoiced according to additional Purchase Orders.

The subscription packages can only be increased but not reduced during the contract period.

Due to the cancellation policy, a customer can only reduce the number of subscribed packages if the framework contract subscription expires.

Billing

A customer who has subscribed to Virtual Assist will be charged upfront on a yearly basis according to the numbers and types of subscription packages subscribed to.

Annex 2

CLOUDSTRUCTURE AS A SERVICE Conditions of Third Parties

Terms of use of the Third Parties:

https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=17585

https://azure.microsoft.com/de-de/support/legal/sla/kubernetes-service/v1_1/

https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Annex 3

ASMPT Privacy Statement

Regarding ASMPT Privacy Policy please refer to documents provided under the following link:

https://smt.asmpt.com/en/privacy-policy/

Annex 4

Data Processing Agreement
pursuant to Art. 28 GDPR

1 Preamble

This agreement establishes the tasks and duties to be performed by the contracting parties in accordance with Art. 28 of the General Data Protection Regulation (GDPR).

In order to use the IoT applications (e.g. Virtual Assist, FactoryTwin, FactoryChat, etc.) of the processor, the parties agree that an agreement governing the processing of personal data is required for this. For applications in which no personal data is processed, no further specifications are made in the paragraphs below.

2 Subject and Duration of Processing

2.1 Subject of Processing

The commissioned data processing shall be carried out for the execution of the following tasks by the processor (definition of tasks):

The IoT applications used by the processor, as indicated in the preamble, shall enable the client to receive information from the processor and record the following data:

- Recording of warnings, errors and maintenance reports for assets in production (production modules);
- Provision of fault solutions by the processor;
- Provision of information supplied by the client (collaboration)
- Evaluation and analysis of the data entered (reporting)

2.2 Duration of Commissioned Processing

The data processing contract shall run for an indefinite period and may be terminated by either party the following month with a notice period of (1) month. This shall have no bearing on their right to terminate the contract without notice. The termination date of the effectiveness of the termination of the main agreement (see §9) also applies to this annex.

3 Substantiation of the Contract

3.1 Type and Purpose of the Envisaged Data Processing

Detailed description of the subject of processing with regards to the scope, nature and purpose of the tasks to be performed by the processor:

- Provision and maintenance of the Cloudstructure;
- Provision and maintenance of the applications (e.g. Virtual Assist, FactoryTwin, FactoryChat, etc.)
- Connection of the client's SMT products (developed by ASMPT) to the applications used
- Connection of products developed by other manufacturers (third-party providers) to the applications used, provided this has been specifically requested

Data shall be processed and used exclusively within the Federal Republic of Germany, a Member State of the European Union or another state within the European Economic Area. If the processor is asked to transfer or disclose personal data from this processing contract on the basis of a judgement issued

by a court in a third country or a decision issued by an administrative authority in a third country (Art. 48 GDPR), the processor shall immediately notify the controller. The same applies to any third-country judgements or administrative decisions issued against subcontractors.

The controller must give its written permission for data processing to be carried out in a third country – or for the data to be otherwise transmitted to a third country – and this may only occur if the special requirements stipulated in Art. 44 GDPR are met.
If a subcontractor is to be commissioned, these requirements shall apply in addition to the provisions stipulated in Section 7.
At the time the contract is concluded, the data shall be hosted at the Microsoft Azure Data Centre near Amsterdam.

3.2 Type of Data

The following types / categories of personal data shall be processed (list / description of the data categories):

- Personal master data (e.g. first name, last name, title, form of address)
- Contact details (e.g. phone number, email address)
- Planning and control data
- Online data (e.g. IP address, computer name)
- Image data

3.3 Category of Data Subjects

The following category of data subject shall be affected by the use of personal data within the scope of this contract (list / description of the categories of data subjects):
The controller's "employees" within the meaning of this agreement are:

1. workers, including temporary agency workers in relation to the user worker,
2. employees for their vocational training,
3. participants in benefits for participation in working life as well as in assessments of professional aptitude or work trials (rehabilitators),
4. employees in recognised workshops for disabled people,
5. persons who, because of their economic dependency, are to be regarded as persons similar to employees; these include homeworkers and persons treated as such;

Applicants for an employment relationship and persons whose employment relationship has ended are considered employees.

4 Rights and Obligations of the Controller

4.1 Authority of the Controller

The data is handled exclusively within the framework of the concluded agreements and in accordance with the documented instructions of the controller, see Art. 28 Para. 3 Sub-Para. 1 Clause 3 point a) GDPR if the processor is not obliged as a result of the law of the European Union or a member state of the European Union to process personal data governed by this contract without or against the instructions of the Client. The processor must notify the controller of any such legal requirements before starting the data processing, unless the legislation in question prohibits such a notification due to an important public interest.

The controller reserves the right to issue extensive instructions on the nature, scope and procedures of data processing within the scope of the contract description made in this agreement, and such instructions may be substantiated through individual instructions. Any changes to the subject of processing and procedures must be coordinated and documented jointly (see Art. 28 Para. 3 Sub-Para. 1 point a) GDPR). The processor may only supply information to third parties or data subjects with the prior written consent of the controller.

The controller shall immediately confirm any verbal instructions in writing or via email (in text form). The processor shall not use the data for any other purposes and in particular shall not be authorised to pass it on to third parties. No copies or duplicates shall be made without the client's knowledge. This does not apply to any back-up copies required to ensure proper data processing or any data required to comply with statutory retention obligations.

The processor must inform the controller immediately in accordance with Art. 28 Para. 3 Sub-Para. 2 GDPR if it is of the opinion that an instruction is infringing the applicable data protection regulations. The processor shall be entitled to refrain from executing the instruction in question until it has been confirmed or changed by the responsible members of staff at the controller's company.

The persons authorised to issue instructions on behalf of the controller and processor are listed in Annex 2.

4.2 Monitoring Rights of the Controller

The controller has the right to carry out the checks envisaged in Art. 28 Para. 3 Sub-Para. 1 point h) GDPR – including inspections - or to arrange to have them carried out by examiners who are to be appointed on a case-by-case basis. It shall be entitled to ensure the processor is complying with the provisions of this agreement in its business by conducting random checks that must generally be announced in good time. The processor agrees to make the relevant evidence available and give the controller any information it requests and requires to fulfill its obligation to control data processing contracts.

With regard to the monitoring obligations in respect of the controller, the processor shall make sure the controller is able to monitor the implementation of the agreed technical and organisational measures to fulfil the monitoring obligations to be assumed by the controller in accordance with point (h) of Art. 28 (3) GDPR in conjunction with point (c) of Art. 28 (3) GDPR before the start of processing and during the contractual term, and to incorporate a process used to regularly inspect, assess and evaluate the effectiveness of the technical and organisational measures to ensure the security of data processing. To this end, the processor shall provide the controller with any evidence it requests to prove the implementation of the technical and organisational measures stipulated in Art. 32 GDPR. Any evidence to prove the implementation of measures that not only concern the specific data processing contract may also be provided by submitting current certificates, reports or excerpts of reports from independent bodies (e.g. auditors, data protection officer, IT security department, data protection auditors, quality auditors), by proving compliance with the approved codes of conduct indicated in Art. 40 GDPR, by proving a suitable level of certification obtained via an IT security or data protection audit (e.g. according to the basic protection recommended by the Federal Office for Information Security) or by presenting data protection seals and marks in accordance with Art. 42 GDPR, provided such evidence adequately proves the implementation of the technical and

organisational measures in question. This shall have no bearing on the rights granted to the controller in the first paragraph of Section 4.2 above.

5 Rights and Obligations of the Processor

5.1 Rectifying, Blocking and Deleting Data & Handling and Implementing the Rights of Data Subjects

The processor may only rectify, delete or block the data processed within the scope of the contract if instructed to do so by the client.

If a data subject contacts the processor directly, referring to the rights described in Chapter III of the GDPR or specific data subject rights granted by the applicable laws of a Member State of the European Union, the processor shall immediately forward the request to the controller for inspection and processing. It shall not be entitled to respond to such requests independently without consulting the controller. The processor must help the controller – on request and free of charge – to respond to any requests and rights asserted by data subjects.

If covered by the scope of the services and specified in the documented instructions issued by the client, the contractor must directly ensure a deletion concept, the right to be forgotten, the right to rectification, the right to data portability and the right of access.

5.2 Other Processors (Subcontracting)

If the processor would like to contract other processors ("sub-processors") to process or use the personal data of the client, this shall only be permitted under the following conditions:

- Other processors may only become involved with the prior separate or general written approval of the controller, unless they are already listed in this section.
- The processor must impose the same data protection obligations on the other processor as those established in this data processing agreement by way of a contract or another legal act under Union law (Art. 28 GDPR) or German law, in particular providing sufficient guarantees that the technical and organisational measures established herein will be implemented in such a manner that the data processing meets the requirements of the GDPR.
- If the other processor fails to fulfil its data protection obligations, the processor shall be liable to the controller for the fulfilment of the other processor's obligations.
- If another processor is contracted, the controller must be granted the right to audit and inspect the other processor under the terms of this agreement and in accordance with point (h) of Art. 28 Para. 3 Sub. Para. 1 Clause 2 GDPR. This also includes the controller's right to present the processor with a written request for information on the essential content of the contract and the implementation of data protection obligations within the subcontracting relationship – if necessary by inspecting the relevant contract documents.
- If the client has granted the contractor general authorisation to contract other processors, the contractor must inform the client whenever it intends to contract or replace such processors. In such cases, the client may prohibit a processor from being contracted or replaced.
- If another processor fails to fulfil these obligations, the processor shall be liable to the client for the fulfilment of the other processor's obligations.

The following sub-processors have currently been approved for processing data within the scope of the contract:

Subcontractors of ASMPT:

Company	Adress	Partial Supply	EU SCCs / Link
KNOWRON GmbH	Agnes-Pockels-Bogen 1 / 80992 München, Germany	Application Provider	In EU
Microsoft Corporation	One Microsoft Way Redmond, Washington, WA 98052-6399, USA	Provision of optional cloud platform	In EU / General Data Protection Regulation (GDPR) | Microsoft Learn

Subcontractors of KNOWRON GmbH:

Unternehmen	Anschrift	Teilleistung	EU SCCs / Link
Amazon Web Services	Amazon Web Services EMEA, SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg	Cloud-Hosting der App-Server sowie Datenbanken (Standort Frankfurt)	Ja / https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
Google, LLC	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043	Übersetzen der GPS-Koordinaten in Land des Zugriffs, Spracheingaben auf Android-Geräten transkribieren	Ja / https://cloud.google.com/terms/data-processing-terms
IPdata, LLC	IPdata, LLC, 2035 Sunset Lake Road Suite B-2, Newark, Delaware	Übersetzen der IP-Adresse in Land des Zugriffs	Ja / https://ipdata.co/assets/pdf/ ipdata DPA.pdf
Hotjar Ltd.	Hotjar Ltd., Level 2, St Julians Business Centre, 3, Elia Zammit Street, St Julians STJ 1000, Malta, Europe	Erfassen von Besucherstatistiken	Ja / https://help.hotjar.com/hc/en-us/articles/360046543713-Legal-FAQs
Apple Inc.	Apple Inc. One Apple Park Way, Cupertino, California, USA, 95014	Spracheingaben auf iOS-Geräten transkribieren	Ja / https://www.apple.com/legal/enterprise/data-transfer-agreements/datatransfer-ee.pdf
Elasticsearch AS	Elasticsearch AS, Postboks 539, 373 Asker, Norway	Bereitstellen von Cloud-Infrastruktur zum Betrieb einer Suchmaschine (Standort Frankfurt)	In EU
MongoDB Ltd.	MongoDB Ltd., Building Two, Number One Ballsbridge, Ballsbridge, Dublin 4, Ireland	Bereitstellen von Cloud-Datenbanken (Standort Frankfurt)	In EU / https://www.mongodb.com/technical-and-organizational-security-measures
Heroku, Inc.	415 Mission Street, Suite 300, San Francisco, CA 94105	Bereitstellen von Web-Servern (Standort Frankfurt)	Ja / https://devcenter.heroku.com/ articles/gdpr

Notification of Violations by the Processor

The processor shall notify the controller immediately (i.e. within 24 hours) if the applicable regulations for the protection of the controller's personal data or the stipulations established in this contract are violated by the processor itself – or by its employees or sub-processors – or if such violations cannot be ruled out. The minimum content of such notifications is stipulated in Art. 33 (3) GDPR.

The parties are aware that data breaches may result in an obligation to provide information in accordance with Art. 33 & 34 GDPR, particularly following the loss, unlawful transmission or unlawful acquisition of personal data. Therefore, such incidents, regardless of the cause, must be reported to the controller immediately – and if possible within 24 hours – providing the minimum information specified in Art. 33 (3) GDPR. This shall also apply in the event of serious operational disruptions, other suspected violations of regulations for the protection of personal data and any other irregularities in the handling of the controller's personal data. The processor must consult with the controller to take suitable measures to secure the data and mitigate any negative consequences for data subjects. If the controller is subject to obligations in accordance with Articles 33 and 34 GDPR, the processor must support him in this.

5.3 Deletion of Data and Return of Disks

No copies or duplicates of the data shall be made without the client's knowledge. This does not apply to any back-up copies required to ensure proper data processing or any data required to comply with statutory retention obligations.

Once the contractually agreed work has been completed – or earlier if requested by the controller – and, at the latest, when the service agreement is terminated, the processor must return to the controller all documents acquired, all work results created from its processing and usage of the data, and all data and back-ups related to the contractual relationship or, if agreed beforehand, it must delete or destroy the same in accordance with data protection law (point (g) of Art. 28 (3) (1) GDPR). The same applies to any test and scrap material (electronic or in paper form). A deletion log must be presented upon request. Any documentation that serves as evidence to prove that data processing has been carried out properly within the scope of the contract must be kept by the processor beyond the term of the contract in accordance with the applicable retention periods. It may relieve itself of this obligation by handing over such documentation to the controller at the end of the contract.

If the data cannot be deleted by the contractor due to a legal obligation, the contractor shall provide the client with appropriate evidence of its legal obligation and evidence of the measures taken to ensure the security of the client's data.

5.4 Other Obligations of the Processor

The processor shall also assume the following obligations in relation to the processing to be carried out on behalf of the controller:

- It shall appoint a data protection officer in writing, who will be able to perform his/her tasks in accordance with Art. 37-39 GDPR. The contact details of the data protection officer shall be shared with the controller upon request to facilitate direct contact.
  If the contractor is based outside the European Union, it shall appoint the following representative for the European Union in accordance with Art. 27 (1) GDPR:

Company / Organisational Unit	Last Name	First Name	Email
ASMPT GmbH & Co. KG	Pacholik	Markus	datenschutz@asmpt.com

- It shall ensure that the persons authorised to process personal data are obliged to maintain secrecy in accordance with point (b) of Art. 28 Para. 3 Sub. Para. 1 Clause 2 GDPR. Any persons who might gain access to the controller's personal data within the scope of the contract must be obliged to maintain data secrecy or, following the enforcement of the GDPR, to comply with the confidentiality obligations stipulated therein, and they must be informed about their specific data protection obligations arising from this contract and their obligation to observe instructions and keep to the intended purpose. This also applies to any personal data transmitted to the controller by its external service providers for the execution of this contract.
- It shall implement and observe all technical and organisational measures required for the processing in accordance with Art. 32 GDPR.
- It shall support the controller with suitable technical and organisational measures when responding to requests submitted by data subjects to exercise their rights.
- It shall consider the nature of processing and the information available to assist the controller
  - in ensuring the security of processing in accordance with Art. 32 GDPR;
  - in reporting personal data breaches in accordance with Art. 33 GDPR;
  - in notifying the data subjects affected by a personal data breach in accordance with Art. 34 GDPR; this shall be done exclusively by the client, unless the contractor has been declared the sole controller in accordance with Art. 28 (10) GDPR (see Section 7);
  - in conducting data protection impact assessments in accordance with Art. 35 GDPR; and
  - in conducting a prior consultation with a supervisory authority in accordance with Art. 36 GDPR.
- It shall assist the controller with monitoring and measures conducted within the scope of the contract and with cooperation requests submitted by supervisory authorities.
- It shall immediately inform the controller about any inspections and measures taken by the data protection supervisory authorities. This also applies if a responsible authority as defined by the Federal Data Protection Act is conducting the inspections at the processor's premises.
- It shall monitor the contract by checking its execution and fulfilment, particularly regarding compliance and, if necessary, the adjustment of regulations and measures for the processing.
- It shall ensure the traceability of the technical and organisational measures and provide the controller with all the information it needs to prove compliance with the obligations stipulated in Art. 28 GDPR. The processor may fulfil this obligation by presenting current certificates, reports or excerpts of reports from independent bodies (e.g. auditors, data protection officer, IT security department, data protection auditors, quality auditors), by proving compliance with the approved codes of conduct indicated in Art. 40 GDPR, by proving a suitable level of certification obtained via an IT security or data protection audit (e.g. according to the basic protection recommended by the Federal Office for Information Security), or by presenting data protection seals and marks in accordance with Art. 42 GDPR, provided such evidence adequately proves the implementation of the agreed technical and organisational measures and such measures not only concern the specific data processing

contract. This shall have no bearing on the controller's right to conduct on-site inspections, as described in Section 4.2 above.

- The contractor shall assist the client in the fulfilment of its obligations stipulated in Art. 12, points (e) and (f) of Art. 13 (1), points (e) and (f) of Art. 14 (1), Art. 15, Art. 16 to 20 and Art. 25 GDPR (provided such matters concern applications of the contractor over which the client has no control), and it shall provide the client with all the necessary documents and information.
- It shall document all written instructions received from the client in accordance with point (a) of Art. 28 (3) GDPR.
- The contractor shall provide the client with all logs created in accordance with Section 76 of the German Law for the Adaptation and Implementation of Data Protection Law in Line with European Regulations (DSAnpUG), in order to prove the fulfilment of its obligations.

6 Security of Processing

The technical and organisational measures described in Annex 1 have been defined as binding between the controller and processor.

The processor shall ensure the measures allow data to be processed in accordance with the GDPR and any other applicable legal requirements in a Member State of the European Union, and that they guarantee the protection of the rights of data subjects. The processor hereby declares that the technical and organisational measures shall ensure a suitable level of protection against the risks posed to the rights and freedoms of natural persons during data processing; it shall guarantee this by considering the probability and severity of such risks, the current state of technology, implementation costs and the type, scope, circumstances and purposes of data processing.

Some of the measures to be taken shall not be specifically for this contract (e.g. those regarding confidentiality, integrity, availability, capacity, recoverability, transparency, non-linkability and processes for the regular inspection and evaluation of the effectiveness of the technical and organisational measures), while other measures shall be specifically for this contract (e.g. those regarding the nature of the data exchange / provision of data, nature / circumstances of the processing / data storage and nature / circumstances of output / data transmission).

The technical and organisational measures shall be subject to technical developments and progress. In this respect, the processor shall be obliged to regularly check whether the measures are up to date and to adapt existing measures or implement new measures in line with the state of the art. It shall particularly consider the guidelines, advice and recommendations of the data protection supervisory authority. When adapting the established measures, the security level must not drop below the agreed level. Significant changes must be documented. The processor shall keep a suitable record in accordance with Art. 30 (2) GDPR and, at the request of the controller, it must provide all information required to keep a record in accordance with Art. 30 (1) GDPR. The exceptions indicated in Art. 30 (5) GDPR shall not apply in connection with this agreement.

When identifying sufficient guarantees in accordance with Art. 28 (1) and (4) GDPR, the controller shall also consider evidence of compliance with approved certification procedures (Art. 42 GDPR) and observance of approved codes of conduct (Art. 40 GDPR). Any such evidence shall be included in Annex 1 if it sufficiently and specifically reflects the technical and organisational measures and is accepted by the controller. The processor must immediately inform the controller about any changes to the certification content. If the processor loses its certification, it must inform the controller within 24

hours and explain in writing how the requirements for the security of processing are met in accordance with Art. 32 GDPR.

7 Sole Responsibility

If the processor infringes the GDPR by determining the purposes and means of processing, such as by violating this data processing agreement and/or any instructions issued by the client on the basis of this agreement, it shall become solely responsible for the data processing and shall bear all associated responsibilities (see Art. 28 (10), Art. 82 (1) and Art. 79 (2) GDPR).

8 Rights of Retention

Under no circumstances may the processor assert rights of retention with regard to the client's data.

9 Entry into Force

This agreement shall enter into force on the date it is signed.

10 Final Provisions

10.1 By way of derogation from Art. 28 (9) GDPR, any amendments or additions to this agreement must be made in writing, as described in Section 126 of the German Civil Code (BGB). This also applies to the amendment of this clause. The written form may only be replaced by the electronic form under the conditions specified in Section 126 (3) BGB and Section 126a BGB. No verbal side agreements have been made.

10.2 If a data protection supervisory authority or a court believes that

- the collection, processing and/or use of data within the scope of this contract;
- provisions stipulated in this agreement or the absence of certain provisions; or
- the agreed technical and organisational measures or the absence of certain technical and organisational measures

constitutes a violation of European or German data protection law, the parties shall act in good faith to negotiate an amendment / addition to this agreement and/or the procedure to remove the identified deficiencies.

10.3 If amendments or additions to this agreement become necessary or obvious as a result of legislative changes, the parties shall act in good faith to negotiate the required amendments / additions to this agreement. This shall also apply if the processing procedure itself has to be changed to comply with legal regulations. Sentences 1 and 2 shall not apply to any conditions that go beyond the statutory requirements but are not prohibited by law.

10.4 The obligations to negotiate amendments or additions to this agreement and/or the procedure, as stipulated in Sections 10.2 and 10.3, shall not apply if the deficiencies in question can be removed through the client's right to issue instructions.

10.5 If the data protection supervisory authorities publish recommendations, guidelines or best practices that are applicable to the data processing covered under this agreement, the processor shall proactively check whether the directives are incorporated in its current procedure and, if this is not the case, the processor shall suggest relevant changes to the controller.

10.6 If the processor incurs additional expenses as a result of amendments or additions made on the basis of Sections 10.2 to 10.5 of this agreement, the parties shall act in good faith to agree on the

distribution of the additional costs. This shall not apply if the processor also has to make the adjustments for other clients. The processor must therefore proactively state whether the negotiated adjustments are being – or have been – made for other clients.

10.7 If a data protection impact assessment has to be submitted for the data processing covered under this agreement as a result of current or future statutory provisions, requests for information or orders issued by supervisory authorities or judicial proceedings, the processor shall provide the controller with a data protection impact assessment free of charge. If the processor has already conducted a data protection impact assessment but it does not meet the requirements or necessary content stipulated by the GDPR, the processor shall conduct a new data protection impact assessment free of charge in accordance with the valid statutory provisions and submit it to the controller.

10.8 If the parties cannot agree within an appropriate period of time, at the latest however three months after the request for negotiations about any changes or additions as defined in points 10.2 and 10.3, both parties are entitled to an extraordinary right of termination, both with regard to this agreement and with regard to the service agreement as defined in point 2.1. The controller shall also be granted such a right of termination if the processor cannot or will not implement any recommendations, guidelines or best practices published by the data protection supervisory authorities. In general, neither party may claim compensation for expenses or damages (e.g. due to loss of profit) or contractual penalties for premature termination. This shall not apply if any of the following events give rise to termination:

- A contractual guarantee is violated, or the negotiations described in Sections 10.2 and 10.3 break down due to a violation of the principles of good faith; or
- The client refuses to implement recommendations, guidelines or best practices published by the data protection supervisory authority.

10.9 The parties agree that the provisions of this agreement are not the general terms and conditions of a party. Rather, the parties agree that this agreement has been negotiated individually.

10.10 In the event of any conflicts between this agreement and the service agreement described in Section 2.1, this agreement shall take precedence. If this agreement is found to contain conflicting provisions, the more favourable provision shall apply from the point of view of the controller or data subjects.

Annex 1 to the Agreement pursuant to Art. 28 GDPR

General Technical and Organisational Measures pursuant to Art. 32 GDPR to Ensure the Security of Processing (provided by ASMPT)

The following list applies exclusively to the processing of personal data carried out by the processor itself.
The technical and organisational measures of subcontractors are not explicitly listed here.

1 Pseudonymisation and Encryption

The following measures are implemented to ensure pseudonymisation and encryption:

- Transport encryption
- Email encryption
- Disk encryption
- Remote access and maintenance exclusively via VPN connection
- Pseudonymisation / anonymisation of test data or in test environments

2 Confidentiality

The following measures are implemented to ensure confidentiality:

- Definition of a concept for the assignment of necessary rights and roles on the basis of an ASMPT identity management system and a secure authentication method
- Limitation of authorisations to employees who have no professional conflicts of interest and are demonstrably responsible (local, technical), technically qualified, trustworthy (possibly subject to a security check) and formally approved
- Definition and monitoring of the use of approved resources, especially communication channels
- Specified environments (buildings, rooms) that are adequately equipped for the process
- Definition and monitoring of organisational processes, internal regulations and contractual obligations (obligation to maintain data secrecy, non-disclosure agreements, etc.)
- Encryption of saved or transferred data, and processes for the management and protection of cryptographic information (cryptographic plan)
- Protection against external influences (espionage)
- Documentation of the access control system
- Existence of automated access control systems
- Maintenance and management of automated access control systems
- Access / exit log
- Evaluation of access logs
- Specific purpose of stored log-in details
- Restricted access to certain areas for service providers
- Building security concept
- Security zones in the building security concept
- 24/7 security service
- Access security through building technology

- Existence of non-automated access controls
- Retention period for access logs
- Staff ID cards (worn visibly)
- Logging of badges issued to visitors and companies
- Validity period of code cards for external visitors
- Reception during business hours
- Visitor list
- Visitor badges
- Policy for dealing with visitors
- Lock and key regulations
- Access control rules (incl. logging and evaluation of user access; the frequency of controls depends on the stored data)
- User registration
- Rules for the use of network services
- Access controls specifically for the wireless network
- Penetration and security tests
- Identification / authentication of external maintenance personnel
- Password management
- Remote maintenance regulations
- Antivirus / spam filter
- Regulations for a secure workplace (e.g. BIOS password, BitLocker, automatic desktop log-out, etc.)
- Encryption / tunnelling (VPN = virtual private network)
- Logging of external access, incl. regular check of authorisations (the frequency of the check depends on the systems and the criticality of the data)
- Regulations for secure transmission
- Data classification
- Documentation of programmes for automated exchange procedures
- Logging of automated exchange procedures
- Pseudonymisation (point (a) of Art. 32 (1) GDPR; Art. 25 (1) GDPR) The processing of personal data in such a way that the data can no longer be matched to a specific data subject without the use of additional information, provided this additional information is stored separately and subject to suitable technical and organisational measures
- Clear desk and clear screen regulations
- Use of secure encryption algorithms
- Mobile device management
- Mobile device policy

3 Integrity

The following measures are implemented to ensure integrity:

- Restriction of writing and editing rights
- Use of checksums, electronic seals and signatures in data processing according to a cryptographic concept
- Documented assignment of rights and roles
- Processes to keep data up to date

- Definition of the desired flow of processes and regular tests to determine and document their functionality, risks, vulnerabilities and side effects
- Logging of processes
- Evaluation of log files
- Protection of log data
- Definition of the purpose of log files
- Logging of user behaviour following the detection of security breaches
- Definition of responsibilities
- Documentation of instructions (in writing)
- Identity checks
- Monitoring of contractual performance (incl. briefing employees on their contractual duties)
- Controlling data transfers

  No unauthorised reading, copying, altering or deleting during electronic transfer or transport e.g. encryption, virtual private networks (VPNs), electronic signature

4 Availability

The following measures are implemented to ensure availability:

- Creation of back-up copies of data, process statuses, configurations, data structures, transaction histories, etc. according to a tested concept
- Protection against external influences (malware, sabotage, force majeure)
- Documentation of data syntax and semantics
- Redundancy of hardware, software and infrastructure
- Implementation of repair strategies and alternative processes
- Regulations for the substitution of absent employees
- Controlling availability

  Protection against accidental or deliberate loss or destruction, e.g. back-up strategy (online / offline; on-site / off-site), uninterruptible power supply (UPS), antivirus, firewall, reporting channels and emergency plans
- Safe disposal of paper and disks
- Safe disposal of disks and devices containing storage media
- Flood protection
- Separation of electrical circuits
- Computer rooms located in separate fire compartments
- Avoidance of flammable or unprotected areas linking separate fire compartments
- Restriction of access to the IT area (e.g. video surveillance and alarms)
- Air conditioning documentation
- UPS systems
- Surge protectors
- Lightning rods
- Early warning system for fire detection
- Regular maintenance of the fire alarm system
- Fire extinguishers
- Training of specific employees in firefighting
- Existence of a back-up data centre
- No sanitary facilities located in or above the server room

5 Capacity

The following measures are implemented to ensure capacity:

- Performance monitoring
- Pre-selection of appropriate performance indicators, incl. regular reviews
- Long-term evaluations (retrospective and anticipatory) for the development of appropriate measures

6 Recoverability

The following measures are implemented to ensure recoverability:

- Back-up procedures
- Mirroring of hard drives, e.g. RAID method
- Uninterruptible power supply (UPS)
- Separate storage of back-up media in safe places
- Antivirus / firewall
- Emergency management
- Business continuity management systems
- Contingency plans (e.g. information and recovery plans)

7 Transparency

The following measures are implemented to ensure transparency:

- Documentation of procedures, incl. aspects of business processes, databases, data flows, IT systems used, operational processes, interaction with other procedures
- Documentation of tests, approval and, if necessary, prior inspection of new or changed procedures
- Documentation of contracts with in-house staff, contracts with external service providers and third parties who collect or receive data, business distribution plans, responsibility regulations
- Documentation of consent and objections
- Logging of access and changes
- Proof of data sources (authenticity)
- Versioning
- Logging of processing methods on the basis of a logging and evaluation plan

8 Non-Linkability

The following measures are implemented to ensure non-linkability:

- Restriction of processing, usage and transmission rights
- Programme-based omission or closing of interfaces in processes and process components
- Regulatory measures for the prohibition of backdoors and quality assurance audits to ensure compliance in software development
- Separation along organisational / departmental boundaries
- Separation of production and test environments
- “Internal multi-client capability” / purpose limitation
- Separation of functions (production / test)
- Separation using role concepts with graded access rights on the basis of an ASMPT identity management system and a secure authentication method

- Approval of user-controlled identity management by the processing body
- Use of pseudonyms, anonymisation services and anonymous log-in details for the specific purpose, and processing of pseudonymised / anonymised data
- Regulated procedures for changes of purpose
- Controlling separation

  Separate processing of data collected for different purposes, e.g. multi-client capability, sandboxing

9 Procedures for the Regular Inspection and Evaluation of the Effectiveness of Technical and Organisational Measures for Secure Data Processing

The following measures are implemented to ensure regular inspections and evaluations:

- IT security concept
- IT security management systems
- IT policies for administrators and users
- Work and process instructions
- Job descriptions
- Regulations for the substitution of critical persons
- Dual control principle
- Rules for the procurement of hardware and software
- Change request process for software / programme changes
- Regular security training for all employees (at least once a year)
- Regular security patrols
- Regular inspection of technical and organisational measures
- Written appointment of a data protection officer
- Written appointment of a central data protection officer
- Written appointment of an information security officer
- Regular data protection training for all employees (at least once a year)
- Record for all processes involving personal data
- Data protection management
- Incident response management
- Default settings to ensure data protection (Art. 25 (2) GDPR)
- Order control

[General Technical and Organisational Measures pursuant to Art. 32 GDPR of Subcontractors listed in 5.2. of Annex 4 can be provided on request]