macmon SDP Terms of Use

between
macmon secure GmbH, Alte Jakobstraße 79-80, 10179 Berlin

- **"macmon"** -

and the Customer

- **"Customer"** -

macmon and the Customer referred to collectively as the "**Parties**" and individually as a "**Party**".

PRELIMINARY REMARK

(A) macmon develops, distributes and operates software to improve the security of computer networks, including the macmon cloud SDP controller and the macmon cloud SDP Gateways (collectively **"SDP Services**").

(B) macmon Secure Defined Perimeter (**"SDP**") enables access to third-party cloud services, cloud data centre Resources and Resources on customer networks from any location flexibly and dynamically by first checking the User's Client and the User itself and then, depending on the result, allowing, restricting or blocking access. The details of the access options can be regulated by an administrator using a management interface (**"SDP Front End**").

(C) macmon does not distribute the SDP Services directly, but indirectly through partners and managed service providers, who in turn are the direct contractual partners of the Customer and sell the SDP Services to the Customer in their own name as their own service. These Terms of Use only stipulate the conditions under which the SDP Services may be used. The partner or managed service provider from whom the Customer has ordered the SDP Services is exclusively responsible towards the Customer.

(D) The Customer intends to use the macmon cloud SDP controller and/or the macmon cloud SDP Gateways and the other Contractual Services in accordance with its Order placed with the partner or managed service provider ("**Order**").

Therefore, the Parties agree as follows:

1. SCOPE

1.1 These Terms of Use govern the provision of and access to the SDP Services and the SDP Front End required to manage and monitor the SDP Services.

1.2 These Terms of Use apply in addition to the Agreement between the Customer and the partner or managed service provider. The partner or

managed service provider remains solely responsible to the Customer for the SDP Services. Partners and managed service providers are not authorised to bind macmon in relation to Customers, to represent macmon in relation to Customers or to change these Terms of Use. Any terms and conditions of the Customer that conflict with, deviate from or supplement these Terms of Use only become binding if macmon has expressly agreed to their application in writing. It is not deemed consent if, with knowledge of the Customer's terms and conditions, macmon accepts contracts, provides services or directly or indirectly refers to letters containing the terms and conditions of the Customer or a third party.

2. DEFINITIONS

The following terms each have the following meaning. Other terms defined in these Terms of Use have the meanings assigned to them there.

2.1 "**BGB**" means the German Civil Code.

2.2 "**Client**" means an end device that provides a connection to the macmon SDP Services in order to use the SDP Services.

2.3 "**Gateway**" means the macmon cloud SDP Gateway operated by macmon and/or a Gateway operated by the Customer and on which the Gateway Software runs ("**Customer Gateway**").

2.4 "**Gateway Software**" means the software developed by or on behalf of macmon, running on the macmon cloud SDP Gateway and offered by macmon to the Customer for download.

2.5 "**Business Day**" means any day from Monday to Friday, excluding public holidays in Germany.

2.6 "**Customer Relationship**" means the relationship between the Customer and macmon, which is either based on

- partner sales, where the Customer receives the SDP Services from one of macmon's partners, or
- managed service sales, where the Customer receives the SDP Services from a managed service provider.

2.7 "**Customer Data**" means all confidential data generated by the Customer or Users when using the SDP Services or the SDP Front End.

2.8 "**Users**" means employees, Customers or other users who wish to use the Customer's infrastructure via the SDP Services.

2.9 "**Resource**" means hosts, services, applications or similar resources on a network.

2.10 "**Affiliated Companies**" means all companies affiliated with the respective Party within the meaning of sections 15 ff. German Stock Corporation Act (*AktG*).

2.11 "**Agreement**" or "Terms of Use" means these Terms of Use together with all Schedules.

2.12 "**Contractual Services**" means all macmon services provided by the partner or managed service provider to the Customer to which these Terms of Use apply, in particular the use of the SDP Services (section 3), access to the SDP Front End (section 4), the Support Services (section 6) and other services (section 7).

3. SDP SERVICES

3.1 The macmon cloud SDP controller contains the SDP Front End to configure the permissions of each User and Client. Authentication of Users and Clients to use the SDP Services is carried out by checking certificates and other unique characteristics to ensure the identities.

3.2 The Gateways only accept connections from Clients securely authenticated by the macmon cloud SDP controller and according to the configured permissions. Once the connection between the Client and a Gateway is established, the respective Gateway allows communication with the Resources defined for the respective User/Client using encrypted tunnels.

3.3 The definition of rules, which the macmon cloud SDP controller applies when authenticating Clients and hosts, is the sole responsibility of the Customer, who uses the SDP Front End for this purpose. macmon has no obligation to check or even adapt these rules. If the Customer Relationship is based on managed service sales, the managed service provider will make these rules and the other configuration of the SDP Services and the Customer should only configure the SDP Services itself after consultation with the managed service provider.

3.4 The use of the SDP Services by the Customer or User is limited to a data volume in the amount of 500 GB per month per User and to a total volume per month in the amount of the product of the number of licensed Users and 500 GB. This includes any data volume that occurs between the Client and the macmon cloud SDP Gateway. If this is exceeded, further user

licences will be charged per month according to the required volume, which will be invoiced in the following month.

3.5 The Customer may only use the SDP Services for the contractually intended purpose.

4. SDP FRONT END

4.1 The SDP Front End allows the Customer to configure the SDP Services. This includes, for example, defining the rules, under which conditions Clients and Users can be authenticated, or which Resources are accessible.

4.2 macmon provides the SDP Front End as a software-as-a-service solution via the internet. The Customer needs its own internet access to be able to access the SDP Front End.

4.3 The Customer receives administrative access data with the Order for SDP Services and will change the access data immediately. By using the administrative access, additional administrators, Users, Clients, Customer Gateways and Resources can be created and configured, and corresponding policies can be defined.

4.4 The SDP Front End has been developed with the current state of web development techniques in mind, so it should run on the latest versions of any commonly available web browser. However, the software is optimised for the latest version of the Google Chrome web browser. This means that the Customer agrees to use this browser if the Customer experiences malfunctions with other browsers.

5. GENERAL PROVISIONS ON SDP SERVICES AND SDP FRONT END

5.1 macmon may change the SDP Services and the SDP Front End at any time, for example by adding new functions or changing existing functions, as long as these changes are reasonable for the Customer. macmon will notify the Customer of any significant change to the software with reasonable advance notice, for example by means of a display in the SDP Front End.

5.2 If expressly agreed in an Order, the SDP Services and the SDP Front End may also be used by the Customer's Affiliated Companies in relation to their Users if the Customer has previously ensured that such Affiliated Companies comply with the provisions of this Agreement and provided that the quantity of Users agreed between the Parties is not exceeded. The Customer is responsible for acts and omissions of Affiliated Companies as if it had

performed or omitted an act itself. Affiliated Companies of the Customer are not entitled to any direct claims against macmon.

6. SUPPORT SERVICES

6.1 If the Customer Relationship is based on partner sales, the following applies:

6.1.1 macmon will support the Customer in using the SDP Services and the SDP Front End and in solving problems arising from use of the SDP Services and the SDP Front End ("**Support Services**"). The Support Services do not include, among other things, the following:

- solutions for network, workplace or environmental errors that are not directly related to or caused by the SDP Services and/or the SDP Front End;
- services at the Customer's premises or otherwise on site, unless expressly agreed between the Parties, in which case the Customer will pay macmon's reasonable out-of-pocket expenses;
- explanations on how to use the SDP Services and/or the SDP Front End, which are also appropriately available in the Documentation;
- training;
- Support Services in the event of incorrect or non-contractual use of the SDP Services and/or the SDP Front End
- Support Services concerning third-party products or services.

6.1.2 macmon provides Support Services after it receives a support request at support@macmon.eu. Support Services are provided in German and English. macmon endeavours to answer support requests within 24 hours on Business Days. macmon is not required to succeed when handling a support request and find the solution to a problem.

6.1.3 macmon provides the Support Services to the Customer as a voluntary service, free-of-charge within the meaning of sections 611 ff. BGB. macmon may discontinue or change the Support Services at any time. The partner or managed service provider is still the Customer's primary contact for questions, support and for solving problems.

6.2 If the Customer Relationship is based on managed service sales, macmon does not provide any Support Services to the Customer.

7. OTHER SERVICES

7.1 macmon provides the Customer with online documentation in German and English ("**Documentation**") explaining the essential functions of the SDP Services and the SDP Front End.

7.2 Upon request of the Customer, and if macmon agrees, macmon will provide supplementary services related to the SDP Services and/or the SDP Front End. Such services will be remunerated separately by the Customer and are not part of this Agreement, but require a separate agreement between macmon and the Customer.

8. RIGHTS TO THE SOFTWARE, CUSTOMER GATEWAY

8.1 The Customer understands that the SDP Services and the SDP Front End contain proprietary and confidential information that is protected by applicable intellectual property laws and other regulations.

8.2 Except for as provided under section 8.3.2, the SDP Services and SDP Front End are not delivered to the Customer and no rights to receive or use the SDP Services or SDP Front End are granted, whether as a source code or an object code.

8.3 macmon grants the partner or managed service provider the following rights, which the partner or managed service provider transfers to the Customer in accordance with the Order:

8.3.1 macmon grants the partner or managed service provider a simple, non-transferable, non-sublicensable right of access to the SDP Services and the SDP Front End via the internet, limited in time to the term of the Agreement and limited in content to the Customer's internal business purpose. The SDP Services may also be used by the Customer's Users.

8.3.2 In deviation from section 8.2, macmon offers the Gateway Software for download by the Customer and for operating a Customer Gateway. For this purpose, macmon grants the partner or managed service provider a simple, non-transferable right, limited to the term of this Agreement, to install the Gateway Software on a server. Rights to change the Gateway Software are not granted. The partner or managed service provider pays compensation for each Customer Gateway that is connected to a macmon cloud SDP controller. This is based on the Order by the partner or managed service provider, or otherwise on the price lists available from macmon.

9. CUSTOMER'S DUTIES

9.1 The Customer will support macmon appropriately in the performance of Contractual Services.

9.2 The Customer will not disclose the access data for the SDP Services and the SDP Front End to third parties and will exercise the utmost care in safekeeping such access data. The Customer is aware that macmon cannot be held liable for access by third parties in connection with the loss of access data by the Customer.

9.3 Except as permitted in each case by applicable law or by express written agreement between the Parties, the Customer will not directly or indirectly (i) reverse engineer, decompile, disassemble or otherwise attempt to discover any source code, object code or material underlying structures, ideas, know-how or algorithms of the Contractual Services, (ii) make any changes to the Contractual Services or the SDP Services or the SDP Front End, create translations of the Contractual Services or the SDP Services or the SDP Front End or create derivative works from the Contractual Services, the SDP Services or the SDP Front End (iii) use the Contractual Services or the SDP Services or the SDP Front End for the benefit of any third party in contravention of this Agreement or (iv) remove any proprietary notices or labels; whereby if the Customer is a managed service provider, third parties for the purposes of this (iii) are not the customers of that managed service provider and this (iv) does not apply.

9.4 The Customer will use the Contractual Services exclusively in accordance with applicable law and in particular will not use the SDP Services for purposes that violate applicable law or the rights of third parties.

9.5 The Customer is aware that incorrect configuration of the SDP Services using the SDP Front End can massively impair access to the Customer's network. It will use extreme care when configuring the SDP Services. Depending on the criticality of the specific purpose of use, for example if life and limb could be endangered due to restrictions of the SDP Services, the Customer will, at its own discretion, use another solution as a backup service for the SDP Services and/or the Customer's Gateway, which can become active immediately if the SDP Services are not available or only available to a limited extent. macmon strongly recommends such a solution as part of a regular security concept.

9.6 The Customer is obliged to only have suitable and trained employees use the SDP Front End and configure the SDP Services and to log any special incidents that occur in a suitable manner. The Customer will make the

Documentation available to these employees before they use the SDP Front End and will ensure that these employees familiarise themselves with the Documentation.

9.7 The Customer is aware that macmon logs access to the SDP Front End on a user-related basis and retains the logs, for example until attacks have been finally clarified, or at least for seven days.

9.8 The Customer will make a daily recoverable Backup of all data that could be affected by errors in or failure of the SDP Services on an independent system (**"Backup"**).

9.9 The Parties are aware that the SDP Services may be subject to export and import restrictions. In particular, there may be licensing requirements and the use of SDP Services or related technologies may be subject to restrictions abroad. The Customer will comply with the applicable export and import control regulations of the Federal Republic of Germany, the European Union and the United States of America, as well as all other relevant regulations. Performance of the Agreement by macmon is subject to the condition that no obstacles which are based on the national and international regulations of export and import law, as well as no other legal provisions, will prevent performance.

9.10 When configuring the SDP Services, the Customer will take sufficient account of the conditions of its network and existing connection requirements. Configurations of the SDP Services that can be made by the Customer will not be made by macmon. The Customer is therefore solely responsible for carrying out these configurations appropriately. The Customer will only use suitable and trained personnel for this purpose.

9.11 If the Customer uses the Gateway Software as a Customer Gateway, it undertakes to always use the latest version of the Gateway Software provided by macmon.

9.12 The Customer will assert any claims or other rights arising from this Agreement exclusively against its contractual partner through which it obtains the SDP Services, i.e. in particular against the respective partner of macmon or the respective managed service provider, and not against macmon.

10. WARRANTY

10.1 The following subsections of this section 10 only apply if the Customer is a partner of macmon or a managed service provider. They therefore do not

apply in particular if the Customer Relationship is based on partner sales or managed service sales; in this case the Customer's warranty rights arise exclusively from the contract between the Customer and the partner or managed service provider and the debtor of warranty rights is exclusively the partner or managed service provider. Irrespective of this, the Customer acknowledges and agrees to the limitations in section 10.5 and section 10.8 and the Availability Rate in section 10.9.

10.2 Unless otherwise expressly agreed in writing, all Contractual Services are services within the meaning of sections 611 ff. BGB. This means that macmon is not responsible for a certain success in the sense of sections 631 ff. BGB and that there are no warranty rights in this respect. Use of the SDP Services (section 3), the SDP Front End (section 4) and the Gateway Software as Customer Gateway (section 8.3.2) are subject to lease law, in each case, as modified by this Agreement.

10.3 During the term of the Agreement, macmon will ensure that the SDP Services and the SDP Front End will be essentially in the agreed quality, that the Customer's use of the SDP Services and the SDP Front End in the contractually agreed scope will not infringe any third-party rights and that the software will be available within the Availability Rate described in section 10.9.

10.4 The quality of the SDP Services, the Gateway Software used as a Customer Gateway and the SDP Front End are determined exclusively by this Agreement. Warranties regarding the Contractual Services in public statements, in particular in advertising or statements by macmon's employees, do not contain any indications of the quality, unless macmon's management has expressly confirmed them in writing. macmon does not provide any guarantee and does not assume any procurement risk, unless expressly agreed otherwise in writing between the Parties.

10.5 Minor deviations between the SDP Services, the Gateway Software used as a Customer Gateway and the SDP Front End and the agreed quality or minor impairments of the usefulness of the SDP Services, the Gateway Software used as a Customer Gateway or the SDP Front End do not constitute defects. This also includes minor malfunctions that only have a minimal effect on the SDP Services, the Gateway Software used as a Customer Gateway or the SDP Front End or that do not disrupt the functionality of the SDP Services, the Gateway Software used as a Customer Gateway or the SDP Front End or only do so to an insignificant extent.

10.6 If a defect is caused by or is present in defective third-party software, including third-party open source software, the Customer's warranty rights will be limited to assigning any rights macmon may have against such third party to the Customer. This does not apply if the defect is caused by improper handling of the third-party software by macmon, for which macmon is responsible.

10.7 If the Customer does not report a defect within one week after it first occurs together with information about its occurrence and the possibility of reproducing the defect, the Customer's rights in connection with such defect are excluded.

10.8 Claims due to defects are excluded insofar as they are based on the fact that the Customer or its end customer

a) exceeds its right of use,

b) makes changes itself to the SDP Services, the Gateway Software used as a Customer Gateway or the SDP Front End or causes or permits third parties to make changes,

c) has not kept the Gateway Software installed on the Customer Gateway up to date, or

d) otherwise uses the SDP Services, the Gateway Software used as a Customer Gateway or the SDP Front End in an improper or inappropriate manner.

10.9 macmon will ensure an availability of the SDP Services and the SDP Front End of 99.8% per month per Availability Period (as defined below) ("**Availability Rate**").

10.9.1 The "**Availability Period**" is Monday to Sunday, 00:00 to 24:00, excluding Maintenance Periods (as defined below).

10.9.2 macmon is entitled to carry out maintenance work a) at least one week in advance (whereby an email notification or warning in the SDP Front End will suffice) and/or b) at any time in the event of troubleshooting work to protect macmon or Customer Data (**"Maintenance Periods**").

10.9.3 The Availability Rate will be deemed not to have been breached if a) access to the SDP Services or the SDP Front End is possible but it does not function correctly, or b) access to the SDP Services or the SDP Front End is not possible due to outages or other unavailability or disruptions due to causes within the sphere of third parties, suppliers or telecommunication providers or otherwise beyond macmon's control.

10.10 The warranty rights in the event of a breach of the Availability Rate are limited to the following; other warranty rights are excluded, whereby the Customer's right to claim damages under this Agreement is not restricted:

10.10.1 If the breach of the Availability Rate continues for more than two consecutive calendar months, the Customer is entitled to terminate the Agreement without notice and, if a usage fee was paid annually in advance, it is entitled to receive all unused credit. The Customer has no other right of termination in connection with a breach of the Availability Rate.

10.10.2 Each time the SDP Services or the SDP Front End are unavailable for more than 30 consecutive minutes during the Availability Rate, the Customer will receive credit of 5% of the usage fee agreed for the SDP Services or the SDP Front End for the relevant month (but not more than 100% of the usage fee per month) if the Customer makes this claim within five Business Days from the moment the unavailability started.

10.11 Other warranty rights, in particular in the event of defects in the functionality of the SDP Services, the Gateway Software used as a Customer Gateway or the SDP Front End, are limited to the following: macmon will endeavour to remedy significant defects in the SDP Services or the SDP Front End within a reasonable period of time. If macmon is unable to remedy a material defect despite two written reminders from the Customer, each with reasonable notice, the Customer will be entitled to terminate this Agreement for cause if it can prove that the defect materially impairs its use of the SDP Services, the Gateway Software used as a Customer Gateway or the SDP Front End. If the Gateway Software is used as a Customer Gateway, the warranty rights are limited to provision of an updated version of such Gateway Software to download.

10.12 Only the statutory warranty provisions and liability provisions set out in sections 599, 600 BGB apply and will prevail in the event that macmon provides access to the SDP Services or the SDP Front End free of charge, for example for demonstration or testing purposes. In particular, macmon does not provide any warranty in this case.

10.13 Warranty claims become statute-barred one year after they arise.

11. TERM AND TERMINATION

11.1 The term of the Agreement is based on the Order. Unless otherwise agreed in an Order, the Agreement may be terminated by either Party with one month's notice.

11.2 The Agreement may only be terminated in its entirety, partial termination is not possible.

11.3 The right of the Parties to terminate the Agreement for good cause remains unaffected. In particular, macmon has good cause for termination if the Customer breaches an obligation under this Agreement and fails to remedy the breach despite a written reminder; in this case, macmon is entitled to demand 80 % of any agreed remuneration that would still have been due up to the point in time at which the Agreement could have been duly terminated. A reminder in the aforementioned sense is not required in the event of serious breaches of this Agreement.

12. LIABILITY

12.1 For each case of slight negligence or simple negligence, each Party will only be liable in the event of breach of contractual duties, the fulfilment of which characterises the Agreement and on which the contractual partner may rely; and the liability is limited to the foreseeable damage typical for such agreements. Sentence 1 does not apply to damage resulting from injury to life, body or health or in cases of mandatory liability, in particular not to liability for cases in which a guarantee for damage has been assumed, in the case of liability under the German Product Liability Act (*Produkthaftungsgesetz*), liability under the GDPR or in the event of fraudulent concealment of a defect. Strict liability irrespective of fault (*verschuldensunabhängige Haftung*) for defects that already existed at the time of conclusion of the Agreement is excluded. Liability for indirect damage, including loss of profit, is excluded.

12.2 Liability pursuant to section 12.1, sentence 1 is limited to a total of EUR 50,000 per calendar year for all damage-causing events occurring in a calendar year.

12.3 As a rule, claims for damages against macmon, its employees or agents become statute-barred two years after they arise. This does not apply to claims for damages that fall under section 12.1, sentence 2.

12.4 The provisions of this section also apply in favour of macmon's employees, agents and subcontractors to whom tasks have been delegated.

12.5 The Customer will indemnify macmon against all claims of third parties in connection with a breach of rights by the Customer upon first request and will also bear any necessary legal defence costs, expenses and costs. macmon may defend itself against third-party claims at its own discretion. The Customer will support macmon in this process to the best of its ability and provide the necessary information without undue delay.

13. CONFIDENTIALITY

13.1 The Parties will treat as confidential and only use for the contractually agreed purpose all information of the other Party and its Affiliated Companies which is subject to secrecy and which is obtained in connection with this Agreement, including information obtained pre-contractually, orally, in writing or in any other form, and in each case business secrets ("**Confidential Information**").

13.2 Confidential Information is in particular, but not exclusively, Customer Data, the software and the amount of the remuneration to be paid to macmon, but not this Agreement or the fact that this Agreement is entered into between macmon and the Customer.

13.3 The Parties must take all necessary and reasonable measures to prevent disclosure of Confidential Information to and/or the exploitation of the Confidential Information by third parties. It is only permissible to disclose the Confidential Information to such employees, staff and external advisors of the Parties who are directly involved in performance of the Agreement ("need to know"). If they are not professionally bound to secrecy, they are obliged to comply in writing with the confidentiality obligation within the context of this Agreement, and to the extent permitted by law, also for the time after they leave the company. The disclosure of Confidential Information is also permitted if and to the extent that the Party burdened with the obligation of confidentiality ("**Burdened Party**") is obliged to do so by virtue of a legal provision or official order, has informed the other Party in writing of the intended disclosure and has taken precautions provided for by law and/or reasonable precautions to keep the extent of disclosure as low as possible. Otherwise, disclosure to third parties is only permitted with the prior written consent of the other Party.

13.4 The confidentiality obligations under this Agreement do not apply if and to the extent that the otherwise Burdened Party proves that the information concerned:

a) was already generally known at the time the knowledge was gained or became generally known at a later time and without any breach of the obligations under this Agreement,

b) was already known to the Burdened Party at the time knowledge was gained without any breach of confidentiality obligations,

c) was developed by the Burdened Party independently, i.e. without use of or reference to the Confidential Information,

d) was made available to the Burdened Party by third parties who lawfully obtained the Confidential Information and were authorised to disclose it.

13.5 Upon termination of this Agreement, the Burdened Party will, upon the written request of the other Party, promptly and at its own expense surrender to the other Party or destroy, to the extent feasible with a reasonable effort, all Confidential Information (including all data carriers and copies made by the Burdened Party or third parties) and confirm this to the other Party. This does not apply if and to the extent that the Burdened Party is legally required to keep Confidential Information. The Burdened Party does not have a right of retention.

13.6 The confidentiality obligations under this Agreement end five years after this Agreement ends.

14. DATA PROTECTION

The Contract Data Processing Agreement attached to this Agreement as Schedule 1 applies to all processing of personal data by macmon (Processor) on behalf of the Customer (Controller) and takes precedence over the main part of this Agreement.

15. MISCELLANEOUS

15.1 The Customer is (a) only entitled to set-off insofar as its counterclaim is either (aa) undisputed or (bb) declared final and absolute; (b) only entitled to assert a right of retention insofar as its counterclaim is either (aa) undisputed or (bb) declared final and absolute.

15.2 This Agreement and its interpretation and all non-contractual obligations in connection with it are governed by the substantive law of the Federal Republic of Germany. The UN Convention on Contracts for the International Sale of Goods (CISG) does not apply.

15.3 Any amendments and additions to this Agreement must be in written form to be valid. Sentence 1 also applies to any amendment to this clause.

15.4 If the Agreement requires written form, a simple email will suffice, unless otherwise specified.

15.5 The Schedules to this Agreement form an integral part of this Agreement. In the event of any conflict between the provisions of the Schedules and the provisions in the main part of this Agreement, the provisions in the main part of this Agreement will prevail over the provisions in the Schedules, except for Schedule 1 (Data Protection) which will always prevail.

15.6 Should individual provisions in this Agreement be or become void or invalid in whole or in part, this will not affect the validity of the other provisions. Statutory law (section 306 (2) BGB) will apply in place of any general terms and conditions which are either not included or which are invalid. In all other respects, the Parties will agree on a valid provision to replace the void or invalid provision that reflects as closely as possible the original economic purpose, provided that no supplementary interpretation of the Agreement takes precedence or is possible.

15.7 This Agreement and all its Schedules contain all agreements and declarations of the contracting Parties with regard to the subject matter of the Agreement. It supersedes all previous agreements and understandings, oral or written declarations of intent and or other legally binding or non-binding arrangements and side agreements between the Parties in respect of the subject matter of the Agreement.

15.8 The exclusive place of jurisdiction for all disputes arising from or in connection with this Agreement including its validity is Berlin.

Schedule 1
Data Protection

1. Definitions

In this Schedule 1 ("**Contract Data Processing Agreement**"), the following terms have the following meanings:

"Data Protection Laws" means the data protection laws of the country in which the Controller is located (including Regulation (EU) 2016/679 (General Data Protection Regulation - "**GDPR**")) and any other data protection laws applicable to the Controller in connection with the main agreement.

"Personal Data" means, as defined in the GDPR, information concerning an identified or identifiable natural person that is processed by the Processor in the course of providing services to the Controller pursuant to this Contract Data Processing Agreement.

"Standard Clauses" means the standard contractual clauses for the transfer of Personal Data from a Controller in the European Economic Area to Processors in third countries as set out in the Annex to European Commission Decision 2010/87/EU and supplemented by including the description of the Personal Data and the technical and organisational measures.

"Subcontractors" within the meaning of this provision are third parties instructed by the Processor to provide such services which directly relate to providing the main service. This does not include ancillary services which the Processor uses, for example, as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems.

"**Controller**", "**Data Subject**", "**Personal Data Breach**", "**Processor**" and "**Processing**" have the meanings set forth in the GDPR.

2. Processor's obligation to follow instructions

2.1 The Processor must process the Personal Data in accordance with the instructions from the Controller. A prior written agreement between the Parties is required for any further instructions that would result in Processing outside the scope of this Contract Data Processing Agreement (e.g. if a new purpose for processing is introduced).

2.2 The Processor will only disclose Personal Data to third parties (including authorities, courts or law enforcement agencies) if it has obtained written

permission from the Controller or is required to do so by law. If the Processor is required to disclose Personal Data to a law enforcement agency or other third party, it will notify the Controller prior to such disclosure (unless this is prohibited by law).

3. Processor's Personnel

The Processor will ensure that its employees authorised to process Personal Data have agreed to observe confidentiality by signing a contract. An obligation to observe confidentiality is only necessary if there are not already appropriate legal obligations of confidentiality.

4. Technical and organisational measures

4.1 The Processor must implement and maintain appropriate technical and organisational security measures ("**TOMs**") in accordance with the Schedule to prevent Personal Data Breaches and to be able to provide the support described in section 5.

4.2 The TOMs are subject to technical progress and further development. The Processor reserves the right to change the security measures taken.

5. Exercising rights of Data Subjects

5.1 If the Controller receives requests or notifications from Data Subjects in relation to the Processing of Personal Data ("**Request**"), the Processor will support the Controller in a reasonable manner and provide information upon Request.

5.2 The Processor must correct, delete or block Personal Data if instructed to do so by the Controller.

6. Supporting the Controller

6.1 The Processor will support the Controller in ensuring an adequate level of protection through technical and organisational measures.

6.2 In the event of a Personal Data Breach, the Processor must:

a) inform the Controller without undue delay after the breach has been established;

b) provide the Controller with necessary information, cooperation and assistance regarding the measures to be taken in response to a Personal Data Breach.

6.3 Where a data protection impact assessment ("**DPIA**") is required for the Processing of Personal Data under Data Protection Laws, the Processor will,

upon request, provide the Controller with the information and assistance reasonably required for the DPIA.

7. Deletion and return of Personal Data

7.1 Once the processing services have been completed, the Processor must, as the Controller chooses, either delete or return all Personal Data and delete any copies, unless it is required to continue to store them under applicable law.

7.2 If additional expenses are incurred due to deviating specifications when returning or deleting the Personal Data, they will be borne by the Controller.

8. Information rights and audit

8.1 Upon request, the Processor will provide the Controller with all information or certificates reasonably necessary to demonstrate compliance with the obligations set forth in this Contract Data Processing Agreement.

8.2 If the Processor does not provide sufficient information or certificates, or if required by Data Protection Law or by a competent authority, the Processor must enable and cooperate in the on-site audit of the Processor's Processing of Personal Data during normal business hours with reasonable notice. Such audit may not interfere with the Processor's business operations.

8.3 The Processor will forward to the Controller all requests from national data protection authorities relating to the Processing of Personal Data carried out by the Processor. The Processor will cooperate with the Controller in its dealings with national data protection authorities and audit requests received from them.

9. Obligation to report unlawful instructions from the Controller

The Processor must inform the Controller if it believes that an instruction breaches applicable data protection provisions. The Processor may suspend the implementation of the instruction until it has been confirmed or amended by the Controller. The Processor may refuse to implement instructions that are obviously unlawful. The Processor is not obliged to verify the lawfulness of the Controller's instructions.

10. Subcontracting relationships

10.1 The Controller agrees that the Processor may use subcontractors to carry out certain processing activities with regard to Personal Data.

10.2 The current subcontractors are listed in the Schedule.

10.3 If the Processor engages additional subcontractors or replaces or removes subcontractors, it will (i) inform the Controller of this in good time in advance and (ii) enter into a written contract with the subcontractor which imposes the obligations set out in Article 28 (3) and (4) GDPR on the subcontractor. The Controller may object to the engagement of subcontractors within 30 days in writing with appropriate justification if the engagement of a subcontractor violates this Contract Data Processing Agreement or Data Protection Laws.

10.4 The Processor's contract with the subcontractor must comply with the requirements of the Data Protection Laws, in particular Article 28 GDPR.

10.5 If the subcontractor fails to comply with its data protection obligations under the contract or Data Protection Laws, the Processor is liable to the Controller for performance of the Controller's obligations under the provisions of this Contract Data Processing Agreement.

11. International data transmission

11.1 The Processor will not transfer Personal Data to countries outside the European Economic Area ("**Third Country**") for Processing pursuant to this Contract Data Processing Agreement.

12. Contractual term and termination

12.1 This Contract Data Processing Agreement ends automatically when the main agreement ends. The Controller may exercise its rights under this Contract Data Processing Agreement as long as the Processor processes Personal Data.

12.2 Either Party may terminate the Contract Data Processing Agreement at any time with reasonable notice for good cause if the other Party commits a material breach of duty under this Contract Data Processing Agreement.

12.3 If the Controller objects to the removal or replacement of a subcontractor or to the involvement of a further subcontractors the Processor can stop providing the service to the Controller within four weeks of receipt of the objection and terminate the service agreement without notice and with immediate effect if the Processor cannot be reasonably expected to provide the service without the intended change.

13. Liability

13.1 If claims for damages are asserted against a Party due to the Processing of Personal Data, the Party against whom the claim is filed must inform the other Party without undue delay. This only applies to the Controller if the asserted claim is based on a breach of duty by the Processor.

13.2 The Controller will indemnify the Processor from all claims which third parties assert on the grounds of the breach of their rights against the Processor on the basis of the Processing of Personal Data instructed by the Controller unless the third-party claim is based on the Processing of Personal Data by the Processor contrary to instruction. However, nothing in this Contract Data Processing Agreement limits the liability of a Party for loss based on wilful misconduct or gross negligence of the Party. In all other respects, the liability provisions in the main agreement apply.

14. Miscellaneous

14.1 In the event of a discrepancy the provisions of this Contract Data Processing Agreement take precedence over the provisions of the main agreement between the Controller and the Processor.

14.2 None of the Parties will receive remuneration for performing its duties under this Contract Data Processing Agreement unless this is expressly stipulated in this Agreement or another agreement.

14.3 The Processor may charge reasonable remuneration for support when carrying out an audit at the Processor's premises in accordance with this Schedule. The time and effort required for an audit is generally limited to one day per calendar year for the Processor.

14.4 If "written" consent or other cooperation is required in accordance with this Contract Data Processing Agreement it may also be in text form (e.g. by email).

Annex to Schedule 1

The definitions set out in the Agreement apply to this Schedule.

1. Subject of the data processing

   The Personal Data are the subject of the following data processing: [**OPTION 1**: [FREE TEXT)

   [**OPTION 2**: The data processing and its purposes are described in the main agreement]

2. Categories of Data Subjects

   The following categories of Data Subjects are affected by the data processing:

   If applicable, predefined selection fields:

   ☐ Existing customers

   ☐ Interested parties/potential customers

   ☐ Newsletter subscribers

   ☐ Website users/visitors

   ☐ Applicants

   ☐ Interns/working students

   ☐ Employees (permanent staff, trainees, temporary workers, freelancers)

   ☐ Suppliers/subcontractors/contact persons

   [FREE TEXT

3. Categories of Personal Data

   The following categories of Personal Data are affected by the data processing:

   ☐ Master personnel data (esp. name, address, date of birth, telephone number)

   ☐ Contract master data (for example, contractual relationship, name, address of the contractual partner's staff, etc.)

   ☐ Address data (e.g. street, post office box, postcode)

   ☐ Communication data (e.g. email address, telephone number, mobile phone number)

   ☐ Photographs of Data Subjects

   ☐ Internet protocol address (IP address)

☐ Bank details (e.g. IBAN, BIC)

☐ Employee's salary

☐ Credit reports, creditworthiness and fraud alerts

☐ Information on employment relationship (history)

☐ Order data (from online shop)

☐ Email messages

[FREE TEXT

The following special types of Personal Data are affected by the data processing:

☐ Information on physical and mental health

☐ Information on medical care (e.g. test results, medication)

☐ Biometric identifiers (DNA, finger, iris and voice)

☐ Criminal charges, convictions and court files

☐ Information on sex life or sexual orientation

☐ Ethnic origin

☐ Religious or ideological beliefs

☐ Trade union membership

4. Subcontractor

The Processor intends to use the following subcontractors for the Processing of Personal Data. The Controller consents to the engagement of the following subcontractors in accordance with section:

Name of the subcontractor	**Address**	**Work to be carried out**	**International transmission (if applicable)**
[FREE TEXT	[FREE TEXT	[FREE TEXT	[FREE TEXT
[FREE TEXT	[FREE TEXT	[FREE TEXT	[FREE TEXT

5. Description of the technical and organisational measures

In order to ensure adequate protection of Personal Data through technical and organisational measures, the provider implements the following measures in particular, but not exclusively:

5.1 Information security programme

The Processor must maintain an information security programme that regulates the use of people, processes and technologies in the handling of Personal Data. This includes:

☐ The Processor must appoint one or more security officer(s) responsible for monitoring security policies and procedures.

☐ The Processor offers security training to ensure that employees are aware of security policies and procedures and their respective roles. The Processor will also inform staff of the possible consequences of non-compliance with security policies and procedures.

5.2 Access control

The Processor will ensure that unauthorised persons do not gain access to data processing equipment (in particular telephone systems, databases, application servers and connected hardware) used for the Processing of Personal Data. This includes:

☐ The Processor restricts access to facilities containing information systems for the Processing of Personal Data to authorised staff by checking their IDs.

☐ The premises of the Processor are monitored around the clock by a security service through video surveillance or comparable methods at all access points.

☐ The Processor makes use of appropriate security measures to protect against loss of data due to disruptions such as power failure.

5.3 System access control

The Processor takes measures to prevent the data processing systems from being used by unauthorised persons. This includes:

☐ The Processor maintains and updates a list of all authorised users who have access to Personal Data.

☐ The Processor removes the access of users who are no longer employed by the Processor or who have changed their roles.

5.4 Data access control

☐ The Processor ensures that the IT systems used for data processing only grant authorised users the limited access as specified by their individual access rights. This includes:

- The rights of employees to access personal data is limited to the minimum level necessary for their work tasks.

- Personal Data may only be printed in physically secure areas monitored by the Processor and may only be disclosed to employees who need to know about it.

5.5 Monitoring tasks/contracts

The Processor ensures that the Personal Data are processed in accordance with the Controller's instructions. This includes:

☐ Logging of all activities in the area of data processing; this also includes unsuccessful access attempts or authorisation changes;

☐ Regularly checking systems for information security incidents.

5.6 Availability

The Processor ensures that Personal Data cannot be accidentally lost or destroyed. This includes:

☐ Introducing/providing business continuity plans and tests.

☐ Using regular back-up processes and other measures and testing them regularly to enable rapid restoration of systems critical to operations and data when needed.

☐ Using uninterruptible power supplies (for example: UPS, batteries, generators) to ensure the power supply to data centres.

☐ Provision of sufficient data storage capacities.

☐ Regular testing of emergency processes and systems.

5.7 Data separation

The Processor will ensure that data collected for different purposes is Processed separately. This includes the use of technical options (for example client-friendly or separate system landscapes) to separate the Customers' personal data.

5.8 Workplace security

The Processor will take the following measures to guarantee security of all workplaces which are used for access to systems of the Controller to process Personal Data:

☐ a password-protected keyboard lock/screen lock which is activated automatically after a certain period of inactivity (at the latest after 30 minutes).

☐ antivirus and desktop firewall programs will be installed.

☐ immediate installation of safety patches

☐ use of secure passwords