PERSONAL DATA PROCESSING AGREEMENT

THIS PERSONAL DATA PROCESSING AGREEMENT (hereinafter the "**Agreement**") has been entered into in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter the "**Regulation**") as well as other generally binding regulations

BY AND BETWEEN

Business name _____

with its registered seat at _____,

Registration No.: _____,

registered in the Commercial register maintained by the _____ Court in _____ under File No. _____

(hereinafter as the "**Data Controller**")

AND

AnyDesk Software GmbH,

with its registered seat at Friedrichstr. 9, 70174 Stuttgart,

registered in the Commercial register maintained by the Stuttgart Municipal Court in Division B 741697,

(hereinafter the "**Data Processor**");

(the Data Controller and the Data Processor hereinafter collectively as the "**Parties**" or separately as the "**Party**").

WHEREAS:

A. The scope of business conducted by the Data Controller primarily consists of _____.

B. The scope of business conducted by the Data Processor consists of provision of information technology services.

C. The Parties have entered into a license agreement (hereinafter the "**License Agreement**"), on the basis of which the Data Processor provides to the Data Controller services in relation to the AnyDesk software application (hereinafter the "**Services**").

D. The Data Processor performs personal data processing for the Data Controller by virtue of provision of the Services to the Data Controller under the License Agreement.

E. In terms of the provision of the Services, the Parties wish for their mutual rights and obligations to be performed in a way that the processing of personal data thereof is carried out in accordance with the Regulation and generally binding regulations of the Federal Republic of Germany.

NOW, THE PARTIES HERETO AGREE AS FOLLOWS:

1. Subject of the Agreement and the Purpose of Processing

1.1 This Agreement governs and regulates the relations between the Data Controller and the Data Processor, particularly, the Agreement defines the subject matter and duration of the processing; the nature and purpose of the processing; the type and extent of personal data to be processed; the categories of data subjects; the obligations and rights of the Data Controller and the Data Processor; and conditions and guarantees of the Data Processor from the viewpoint of the technical and organizational security of personal data.

1.2 Whilst performing the License Agreement, the Data Processor processes personal data for the Data Controller for which the Data Controller has identified following purposes of processing:

(i) Provision of the AnyDesk software application and related services including customer support.

1.3 The Data Processor processes personal data in accordance with the Regulation, the generally binding regulations of the Federal Republic of Germany, this Agreement, exclusively for the purposes specified by the Data Controller and per its instructions.

1.4 The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes applicable data protection law. The Data Processor shall then be entitled to suspend the execution of the relevant instruction until the Data Controller confirms or changes it.

2. Scope of Data

2.1. For the purposes of this Agreement, personal data shall mean any information relating to a data subject that is subject to protection under the generally binding regulations and which is received by the Data Processor for implementation of the purpose of processing specified by the Data Controller.

2.2. Under this Agreement, the Data Processor processes the personal data of the data subjects to the following extent (type of personal data):

(i) start of the AnyDesk software application,

(ii) IP-address of the device using the AnyDesk software,

(iii) statistical information about the device using the AnyDesk software (e.g. CPU-type, screen resolution),

(iv) time and duration of AnyDesk software sessions

(v) AnyDesk-IDs of the AnyDesk's session participants.

(hereinafter the "**Personal Data**").

2.3. Under this Agreement, the Data Processor processes the personal data of the following categories of data subjects:

(i) Users of AnyDesk software.

3. Rights & Obligations of the Parties

3.1. Under this Agreement, the Data Controller authorizes the Data Processor to process the Personal Data which the Data Controller provides to the Data Processor for the purposes specified in this Agreement and under the terms and conditions agreed herein, while the Data Processor undertakes to process the Personal Data in accordance with this Agreement, the Regulation and the generally binding regulations of the Federal Republic of Germany.

3.2. The Data Controller guarantees that it demonstrably has the Personal Data at its disposal in accordance with the Regulation and the generally binding regulations of the Federal Republic of

Germany, and, provided it follows so therefrom, has duly awarded consent of data subjects to process their Personal Data as well. Should the data subject revoke the consent to process his or her Personal Data during the term of this Agreement, the Data Controller is obliged, without undue delay, to inform the Data Processor, who shall then cease to process the Personal Data of the data subject and subsequently delete them.

3.3. The Data Controller has determined the following methods and means of processing for the Data Processor:

(i) The Personal Data will be processed by the Data Processor both manually in physical form and electronically, including automated processing;

(ii) The Personal Data will be collected, recorded, stored on data carriers, used, retained, blocked, and disposed of by the Data Processor on the basis of this Agreement.

3.4. The Data Processor shall use the Personal Data in accordance with the arrangements and for the purposes specified in this Agreement. The Data Processor shall not use the Personal Data for any other purpose.

3.5. The Parties have a duty of confidentiality in relation to the content of this Agreement as well as to any information which each Party learns about the other Party during the course of performing its obligations hereunder, except for the cases where the Party is obliged to provide such information under special legal regulation. This duty of confidentiality does not concern publicly known information.

3.6. The Parties are obliged to designate contact persons for the purpose of communication during the term of this Agreement. The list of the contact persons comprises Appendix No. 1 to this Agreement.

3.7. Each Party is obliged, without undue delay, to inform the other Party of any facts learned in connection with the performance of this Agreement that may affect the scope, quality or the timetable for implementation of the activities hereunder.

4. Guarantees of the Data Processor

4.1 The Data Processor shall preserve confidentiality of the Personal Data as well as of security measures taken to ensure the protection thereof, even after the obligations under this Agreement has ceased to exist. The Data Processor shall ensure that its employees and other persons who are involved in the processing of the Personal Data are bound by the same duty of confidentiality throughout the term of this Agreement as well as after it has ceased to exist, and that they are informed about the possible consequences should a breach of this obligation occur.

4.2 When processing the Personal Data, the Data Processor shall especially proceed in accordance with the written instructions of the Data Controller. The Data Processor also guarantees the safety and protection of the Personal Data that are handed over to the Data Processor by the Data Controller in accordance with the Regulation and the generally binding regulations of the Federal Republic of Germany.

4.3 The Data Controller hereby gives its approval to the commissioning of the subcontractors listed in Appendix No. 2 to this Agreement. Any commissioning of subcontractors not included in Appendix No. 2 requires the prior approval of the Data Controller, which shall not be refused without reasonable cause. The prior approval of Controller is deemed to be given, if a) the Data Processor has notified the planned commissioning of a new subprocessor to the Data Controller in writing or in text form, b) the Data Controller has not objected to the planned subprocessing in writing or in text form within seven business days upon receipt of the notification, and c) the Data Processor has entered into a data processing agreement in accordance with the provision 4.4 of this Agreement with the respective subprocessor.

4.4 The Data Processor shall conclude corresponding data processing agreements with the subcontractors. The Data Processor undertakes to set out the data processing agreements with subcontractors in such a way that they reflect the data protection provisions agreed under this Agreement. The Data Controller

has the right to obtain information from the Data Processor, upon written request, on the implementation of the data protection obligations within the subcontract relationship.

4.5 Where a subprocessor fails to fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the performance of the subcontractor's obligations.

4.6 The Data Processor is obliged to take any such technical and organizational measures to prevent any unlawful or accidental destruction, loss or modification as well as any unauthorized disclosure of transmitted, stored or otherwise processed Personal Data, or unauthorized access to them. This obligation shall remain in force even after the processing of Personal Data has been terminated. The technical and organizational measures currently established by the Data Controller are described in Appendix No. 3. The technical and organizational measures are subject to technical progress and further development. In this respect, it is permissible for the Data Processor to change the described technical and organizational measures as long as the security level of the defined measures is not reduced. Upon the Data Controller's request, the Data Processor shall provide the actual technical and organizational measures to the Data Controller.

4.7 The Data Processor shall execute and maintain the Personal Data processing records in accordance with the Regulation vis-à-vis the adopted and implemented technical and organizational measures to ensure the protection of the Personal Data.

4.8 The Data Processor shall ensure that:

(i) persons who process the Personal Data for the Data Processor are informed about the fact that the respective access passwords to any database or storage repository containing the Personal Data should be kept secret and not made available to third parties;

(ii) measures in accordance with Article 32 of the Regulation are in place.

4.9 The Data Processor shall provide the Data Controller with all necessary co-operation:

(i) when the Data Controller is performing its obligation of responding to a request made by a data subject with regard to performance of the data subject's rights (right of access to the Personal Data; the right to portability of the Personal Data; the right to rectification and erasure of the Personal Data; the right to restriction of processing of the Personal Data, the right to object to the processing of the Personal Data), any request made by data subject which is addressed to the Data Processor shall be forwarded by the Data Processor to the Data Controller without undue delay;

(ii) when implementing and maintaining the appropriate technical and organizational measures to safeguard the Personal Data;

(iii) when ensuring compliance with the obligations under Articles 32 to 36 of the Regulation (reporting/notifying breaches of the security of the Personal Data, or alternatively assessing the impact on the protection of the Personal Data, or prior consultation with the Supervisory Authority), the Data Processor shall report a breach of the security of the Personal Data to the Data Controller without undue delay.

4.10 The Data Processor shall enable the Data Controller, or an auditor who has been authorized by the Data Controller, to conduct inspections and audits of the processing of the Personal Data in order to verify whether the obligations for securing the protection of the Personal Data under this Agreement are being performed by the Data Processor (hereinafter the "**Audit**"). The Data Processor shall provide the Data Controller or an auditor who has been authorized by the Data Controller, with any assistance the Data Controller or an authorized auditor might reasonably require in relation to the Audit. The Data Controller will notify the Data Processor of the execution of the Audit in advance within a reasonable time period but no later than one month prior the execution date of the Audit.

4.11 In case that the Data Processor detects a breach of security of the Personal Data, it shall report it, without undue delay, to the Data Controller. A breach of the security of the Personal Data is understood to be a security breach that results in accidental or unlawful destruction, loss, alteration or unauthorized

provision or disclosure of transmitted, stored or otherwise processed Personal Data. This report must include:

(i) a description of the nature of the breach of security of the Personal Data, including, where possible, the categories and approximate numbers of data subjects and categories concerned, and approximate amount of the Personal Data records concerned;

(ii) the name and contact details of the Data Protection Officer or other contact person who can provide further information;

(iii) a description of the probable consequences of the breach of security of the Personal Data;

(iv) a description of the measures that the Data Processor has adopted or proposed aimed at addressing the breach of security of the Personal Data, including any measures for mitigation of the possible adverse impacts.

4.12 The Data Processor shall keep records of all categories of processing activities that are performed for the Data Controller and document material facts that are related to the processing of the Personal Data. This documentation should contain a sufficient level of detail to enable the Data Controller to demonstrate compliance with the Regulation and the Supervisory Authority to conduct a review of compliance of the processing based on these records. These records should contain:

(i) the name and contact details of the Data Processor and the Data Controller, or any potential representative of the Data Controller or the Data Processor and the Data Protection Officer (if any);

(ii) the categories of the processing being performed for the Data Controller;

(iii) information on the transfer of the Personal Data to a third country or international organization, including identifications thereof; and

(iv) further information, if so required by the Regulation.

4.13 The Data Processor shall provide the Supervisory Authority with necessary co-operation when performing its tasks, namely make records of processing activities available during an inspection.

5. Data Processor's Remuneration

5.1. The Parties have agreed that the remuneration for the processing of the Personal Data under this Agreement is included in the remuneration for the Services provided under the License Agreement.

6. Penalties & Liability for Damage

6.1. The Data Processor shall be, in accordance with Article 82 of the Regulation, held liable for any damage caused by the processing of the Personal Data only in case the Data Processor has failed to fulfil the obligations imposed on the Data Processor by the Regulation, or if the Data Processor has exceeded the lawful instructions of the Data Controller or acted contrary to them.

6.2. Liability for damage caused by a breach of obligations under this Agreement is governed by the relevant provisions of German Civil Code ("Bürgerliches Gesetzbuch").

7. Duration of the Agreement and Ways of Termination of an Obligation under this Agreement

7.1. This Agreement has been concluded for the duration of the License Agreement. It shall come into force on the date of its signature by both Parties.

7.2. In case that the obligations under this Agreement are terminated, the Data Processor is obliged, at the choice of the Data Controller, to delete the Personal Data or return the Personal Data to the Data Controller and delete all existing copies. The Data Processor does not have to delete all existing copies of the Personal Data in case their further deposit is required by the EU law or German law.

Furthermore, the Data Processor is not obliged to delete the Personal Data if the Data Processor is lawfully authorized to process the Personal Data for any other purpose; however, the Data Processor shall inform the Data Controller thereof without undue delay after the termination of the obligations under this Agreement.

7.3. Neither Party hereto is entitled to assign any of the rights and obligations under this Agreement to third parties without the prior written consent of the other Party.

8. Final Provisions

8.1. This Agreement is governed by German law. All disputes or claims arising out of or relating to this Agreement shall be subject to the exclusive jurisdiction of the competent courts at the seat of the Data Processor.

8.2. This Agreement supersedes all existing arrangements of the Parties regarding the subject of this Agreement.

8.3. Any amendments to this Agreement must be entered into in writing.

8.4. Documents will be delivered to the addresses of the Parties listed in this Agreement.

8.5. If one or more provisions of this Agreement is invalid, ineffective, void or unenforceable, it shall not result in the invalidity, ineffectiveness, voidness or unenforceability of the entire Agreement. In such case the Parties will substitute such invalid, ineffective, void or unenforceable provision with a provision best-suited to the purpose of such invalid, ineffective, void and/or unenforceable provision.

8.6. This Agreement is executed in two (2) counterparts in the English version. Each of the Parties will receive one (1) counterpart.

List of Appendixes:

1. List of contact persons

2. List of subcontractors

3. Technical and organizational measures

Data Controller _____	**AnyDesk Software GmbH**
In_____ on _____	In_____ on _____
_____	_____
Name and Position	*Name and Position*

APPENDIX NO. 1

List of contact persons

Data Controller _____

Name	**Phone**
	E-mail
Name	**Phone**
	E-mail

AnyDesk Software GmbH

Name	**Phone**
	E-mail
Name	**Phone**
	E-mail

APPENDIX NO. 2

List of subcontractors

philandro Software GmbH

with its registered seat at **Friedrichstraße 9, 70174 Stuttgart**

registered in the Commercial register maintained by the Stuttgart Municipal Court in Division B 743480

APPENDIX NO. 3

List of subcontractors

Technical and organizational measure

Organizational measures:

1. An organization shall have a process for the protection, processing and handling of personal data.
2. Risks associated with the process of protection, processing and handling of personal data are regularly evaluated and the results are regularly presented to management.
3. The organization has an established procedure that immediately responds in the event of a breach of confidentiality, availability, or integrity of the data processed to minimize the negative impact.
4. The organization shall have an authorized person responsible for compliance with the protection, processing and handling of personal data. This role is appointed by the management of the organization.
5. The organization has a process in place to regularly train all employees regarding the protection, processing and handling of personal data. There is documented information about this training.
6. The organization's audit plan regularly includes auditing the process of protecting, processing and handling personal data. The results of the audit are presented to the management and the supervisory board. Audit findings in area of protection, processing and handling of personal data are removed without delay.
7. The organization has an access rights management process in place to minimize access to the data being processed to the extent necessary. This process is regularly audited and the results of the audit are brought to the attention of the Supervisory Board. Audit findings are removed without delay.
8. Before deploying a new version of the application to the production system, it is first tested in a test environment for a defined period. The possibility of misuse of personal data, or the potential reduction of measures already in place against the confidentiality, availability and integrity of personal data, is being tested.

Technical measures:

1. The assets on which the processing of personal data is carried out are in controlled access areas. Only authorized personal organization has access to such spaces
2. Logical accesses are managed and allocated based on roles. The rule to minimize the necessary access by the “need to know” rule is respected
3. The network segment where the data is processed shall be in a separate controlled access network segment.
4. Network segments are separated by Firewall. Firewall settings are evaluated regularly.
5. Use and encrypt data where possible to protect against data compromise. Where is not possible use encryption, pseudo-anonymization is used.
6. An anti-malware solution is deployed on assets (servers and workstations) that is regularly and frequently updated. The environment is regularly scanned with a such anti-malware solution.

7. The retention period for processed data is set, which is regularly evaluated. Backups are checked to see if they are usable in case of an unexpected event and then need to restore the backed-up data.
8. Remote access is strictly managed or forbidden.