DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is entered into by and between:

1. WEMEDOO AG with registered seat at Sumpfstrasse 24, 6312 Steinhausen, Switzerland, CIN: CHE-290.176.074, VAT number: CHE-290.176.074 MWST, (hereinafter: "Processor" or "Wemedoo");

and

2. Client (hereinafter: "Controller" or "Client");

Hereinafter collectively referred to as "Contracting Parties" and individually a "Contracting Party";

WHEREAS:

A. This DPA, which includes the Standard Contractual Clauses adopted by the European Commission, if applicable, reflects the Contracting Parties' agreement with respect to the terms governing the processing of Personal Data under the Agreement (as defined below) via the Tools (as defined below).

B. Annex I and Annex II are an integral part of the DPA and Standard Contractual Clauses.

C. Appendix III is an integral part of the DPA and applies in cases where Personal Data are exported from Switzerland.

D. Appendix VI is an integral part of the DPA and supplements the DPA to address compliance with US Data Protection Laws.

E. This DPA is an amendment to the Agreement and is effective upon its incorporation into the Agreement, which incorporation may be specified in the Agreement or an executed amendment to the Agreement. Upon its incorporation into the Agreement, the DPA will form a part of the Agreement.

F. The term of this DPA shall follow the term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

1. Definitions

"Agreement" means the agreement concluded between the Parties regarding the use of Tool(s), including but not limited to, and as applicable: Wemedoo's General Terms of Service, Product-specific Terms of Service, Acceptable Use Policy, Software as a Service Agreement along with all Appendices attached hereto, and annexes entered into by and between Parties in accordance with the provisions of the governing Master Services Agreement.

"Client" has the meaning ascribed to it in the Agreement.

"Data Protection Law" means all applicable legislation relating to data protection and privacy, including without limitation the EU Data Protection Directive 95/46/EC and all local laws and regulations which amend or replace any of them, including the GDPR and Switzerland Data Protection Act together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time, and US Data Protection Laws. The terms "process", "processing", "processes", "processed", "Data Subject", "Personal Data", "Personal Data Breach", "Controller" and "Processor" will be construed accordingly.

"GDPR" means the General Data Protection 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.

"Instruction" means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available). The parties agree that this DPA and the Agreement (including the provision of instructions via configuration tools) constitute the Client's documented instructions regarding Wemedoo's processing of Personal Data ("Documented Instructions"). Wemedoo will process User Data only in accordance with Documented Instructions.

"Tool(s)" means software owned by Wemedoo which includes:

i. oomnia, which supports clinical trials conducted by Clients and having EDC, RTSM, ETMF, CTMS, and lab management as integrative parts;
ii. ePRO oomnia, which supports clinical trials conducted by Clients and enables patient participation in clinical trials by filling in the available questionnaires; and
iii. eConsent oomnia, which supports clinical trials conducted by Clients by enabling the patients – clinical trial participants – to provide an electronically signed informed consent for participation in clinical trials conducted by Clients.

This DPA applies respectively to all the Tool(s).

"Regulator" means any supervisory authority with authority under the Data Protection Law over all or any part of the provision or receipt of the Service.

"Service" shall have the meaning defined under the corresponding part of the Agreement, provided by the Processor to the Controller via Tools.

"Standard Contractual Clauses" means the clauses pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0915&from=EN

"US Data Protection Laws" means all data or privacy laws in effect in the United States, including the California Consumer Privacy Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer Privacy Act, and the Connecticut Data Privacy Act, all as amended from time to time and as applicable to the processing of personal data under this Agreement.

2. Details of the Processing

a. Categories of Data Subjects. Categories of Data Subjects set out under Annex I.B. of the Standard Contractual Clauses which is attached to this DPA.

b. Types of Personal Data. To the extent to which it is determined and controlled by the Controller in its sole discretion and the extent to which the Controller decides to use functionalities of the Services, types of Personal Data that are processed are set under Annex I.B. of the Standard Contractual Clauses which is attached to this DPA.

c. Subject-Matter and Nature of the Processing. The subject matter of Processing of Personal Data by Processor is the provision of the Services to the Controller via Tool(s) that involve the processing of Personal Data. Personal Data will be subject to those processing activities as may be specified in the Agreement.

d. Purpose of the Processing. Personal Data will be processed for purposes of providing the Services set out, as further instructed by the Controller in its use of the Services via Tool(s), and as otherwise agreed in the Agreement.

e. Duration of the Processing. Personal Data will be processed for the duration of the Agreement, subject to Section 4 of this DPA.

3. Controller's Responsibility

Within the scope of the Agreement and in its use of the Services, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the processing of Personal Data. For the avoidance of doubt, the Controller's instructions for the processing of Personal Data shall comply with the Data Protection Law. This DPA is the Client's complete and final instruction to Wemedoo in relation to Personal Data and any additional instructions outside the scope of DPA will require prior written agreement between the parties. Instructions shall initially be specified in the Agreement and may, from time to time thereafter, be amended, amplified, or replaced by Controller in separate written instructions (as individual instructions, including via email). The Controller warrants that it has an adequate purpose and legal basis for data processing under applicable Data Protection Law. The Controller will demonstrate such purpose and legal basis upon request from Processor.

The Controller shall inform the Processor without undue delay and comprehensively of any errors or irregularities related to statutory provisions on the processing of Personal Data.

4. Obligations of Processor

a. Compliance with Instructions. The parties acknowledge and agree that Client is the Controller of Personal Data and Wemedoo is the Processor of that data. Processor shall collect, process and use Personal Data only within the scope of Controller's Documented Instructions and Data Protection Laws. If the Processor believes that an Instruction of the Controller infringes the Data Protection Law, it shall immediately inform the Controller without delay. If the Processor cannot process Personal Data in accordance with the Documented Instructions due to a legal requirement under any Data Protection Law, the Processor will:

i. promptly notify the Controller of that legal requirement before the relevant processing to the extent permitted by the Data Protection Law; and

ii. cease all processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Controller issues new instructions with which Processor is able to comply.

iii. If this provision is invoked, the Processor will not be liable to the Controller under the Agreement for any failure to perform the applicable services until such time as the Controller issues new instructions in regard to the processing.

b. Security. Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, described under Annex II. The Controller agrees that such measures are sufficient to fulfil the Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR. Such measures include, but are not limited to:

i. the prevention of unauthorized persons from gaining access to Personal Data Processing systems,

ii. the prevention of Personal Data Processing systems from being used without authorization,

iii. ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified, or deleted without authorization,

iv. ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified,

v. ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems,

vi. ensuring that Personal Data is processed solely in accordance with the Instructions,

vii. ensuring that Personal Data is protected against accidental destruction or loss.

Processor will facilitate Controller's compliance with the Controller's obligation to implement security measures with respect to Personal Data (including if applicable Controller's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR), by

(i) implementing and maintaining the security measures described under Annex II,

(ii) complying with the terms of Section 4.d. (Personal Data Breaches); and

(iii) providing the Controller with information in relation to the processing in accordance with Section 6 (Audits).

c. Confidentiality: Processor shall ensure that any personnel whom Processor authorizes to process Personal Data on its behalf is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the above-entitled activities. Wemedoo imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

d. Personal Data Breaches. Processor will notify the Controller without undue delay but within no more than 72 hours after it becomes aware of any Personal Data Breach affecting any Personal Data. At the Controller's request, Processor will promptly provide the Controller with all reasonable assistance necessary to enable the Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Controller is required to do so under the Data Protection Law.

Unsuccessful Security Incidents. Client agrees that:

- an unsuccessful Security Incident will not be subject to this Section 4 (d). An unsuccessful Security Incident is one that results in no unauthorized access to Personal Data or to any of Wemedoo's equipment or facilities storing Personal Data, which includes but does not limit to: pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

- Wemedoo's obligation to report or respond to a Security Incident under this Section 4 (d) is not and will not be construed as an acknowledgment by Wemedoo of any fault or liability of Wemedoo with respect to the Security Incident.

Notification(s) of Security Incidents, if any, will be delivered to one or more of Client's administrators by any means Wemedoo selects, including via email. It is Client's sole responsibility to ensure accurate contact information and secure transmission at all times.

e. Deletion or Retrieval of Personal Data. Processor will keep Personal Data in line with all Data Protection Law and other laws applicable to Processor (e.g. clinical trial regulations). If Controller requires Personal Data processed pursuant to this DPA to be deleted or returned after the termination or expiration of the Agreement, it must inform Processor in writing. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further processing.

Controller shall, upon termination or expiration of the Agreement and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the reasonable measures to return data or to delete stored data. Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by Controller.

5. Data Subject and Regulator Requests

Processor will enable Controller to respond to requests from Data Subjects to exercise their rights under the applicable Data Protection Law in a manner consistent with the functionality of the Service. To the extent that Controller does not have the ability to address a Data Subject request, then upon Controller's request Processor shall provide reasonable assistance to the Controller to facilitate such Data Subject request to the extent able and only as required by applicable Data Protection Law. Controller shall reimburse Processor for the commercially reasonable costs arising from this assistance.

Processor will provide reasonable assistance, including by appropriate technical and organizational measures and taking into account the nature of the processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Law with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subjects to submit their request to the Controller. Controller shall be solely responsible for responding to any Data Subjects' requests.

Unless a Regulator requests in writing to engage directly with Processor the Contracting Parties agree that Controller will handle a Regulator request itself. Controller agrees to keep Processor informed of such communications or correspondence to the extent permitted by applicable law.

6. Audits

Processor shall, in accordance with Data Protection Laws and in response to a reasonable written request by Controller, make available to Controller such information in Processor's possession or control related to Processor's compliance with the obligations of data processors under Data Protection Law in relation to its processing of Personal Data.

Controller may, upon written request and at least 30 days' notice to Processor, during regular business hours and without interrupting Processor's business operations, conduct an inspection of Processor's business operations or have the same conducted by a qualified third-party auditor subject to Processor's approval, which shall not be unreasonably withheld.

Processor shall, upon Controller's written request and on at least 30 days' notice to the Processor, provide Controller with all information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

Wemedoo may at its discretion provide reasonable cooperation to Client in connection with any data protection impact assessment (at Client's expense) or consultations with supervisory authorities that may be required in accordance with Applicable Data Protection Law.

7. Sub-Processors

a. Appointment of Sub-Processors. Controller acknowledges and agrees to (a) the engagement as sub-Processors of Processor's affiliated companies and the third parties, and (b) that Processor and Processor's affiliated companies respectively may engage third-party sub-Processors in connection with the provision of the Service. For the avoidance of doubt, the above authorization constitutes Controller's general written authorization to the sub-processing by Processor.

Where Processor engages sub-Processors, Processor will enter into a contract with the sub-Processor that imposes on the sub-Processor the same obligations that apply to Processor under this DPA. Where the sub-Processor fails to fulfil its data protection obligations, Processor will remain liable to the Controller for the performance of such sub-Processors obligations to the same extent Processor would be liable if performing the Services of the sub-processors under the terms of this DPA.

Where a sub-Processor is engaged, the Controller must be granted the right to monitor and inspect the sub-Processor's activities in accordance with this DPA and the Data Protection Law, including to obtain information from the Processor, upon written request, on the substance of the contract and the implementation of the data protection obligations under the sub-processing contract, where necessary by inspecting the relevant contract documents.

The provisions of this Section 7 shall mutually apply if the Processor engages a sub-Processor in a country outside the European Economic Area ("EEA") not recognized by the European Commission or Swiss Federal Council as providing an adequate level of protection for personal data. If, in the performance of this DPA, Wemedoo transfers any Personal Data to a sub-Processor located outside of the EEA, Wemedoo shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy in respect of that processing is in place.

b. Notification or Objection to New Sub-Processors. The Processor has the Controller's general authorization for the engagement of Sub-processors from an agreed list. The Processor shall specifically inform in writing the Controller of any intended changes of that list through the addition or replacement of Sub-processors and will give the Controller the opportunity to object to the engagement of the new sub-Processors within 10 days after being notified. The objection must be based on reasonable grounds. If the Processor and Controller are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party in accordance with the provisions of the Agreement that regulate term and termination.

8. Data Transfers

Controller acknowledges and agrees that, in connection with the performance of the Services under the Agreement, Personal Data will not be transferred to any country outside the EEA, Switzerland and Serbia, if the Client is established in the EEA. If the Client is established outside the EEA, Personal Data will be transferred to the country of Client's registered seat in addition to the previously mentioned territories. Processor may access and perform processing of Personal Data on a global basis as necessary to provide the Service, in accordance with the Agreement.

The Standard Contractual Clauses will apply with respect to Personal Data that is transferred outside the EEA and Switzerland, either directly or via onward transfer, to any country not recognized by the European Commission Swiss Federal Council as providing an adequate level of protection for personal data (i.e. a third country as described in the Data Protection Law). Therefore, the Standard Contractual Clauses shall apply when the Client is established in a third country. In such case:

i) Module 4 (Processor to Controller) of the Standard Contractual Clauses shall apply.

ii) The parties will complete Annex I, and agree to Annex II, of this DPA in lieu of the Annexes to the Standard Contractual Clauses.

iii) The Standard Contractual Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland.

iv) Any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of Switzerland.

v) The parties agree to Clause 7 (Docking clause) of the Standard Contractual Clauses.

To the extent that Controller or Processor are relying on a specific statutory mechanism to normalize international data transfers and that mechanism is subsequently revoked, or held in a court of competent jurisdiction to be invalid, Controller and Processor agree to cooperate in good faith to pursue a suitable alternate mechanism that can lawfully support the transfer.

9. General Provisions

The Contracting Parties are liable according to the general rules of applicable law, however, Wemedoo is liable according to the scope set out in the Agreement.

Client agrees to indemnify and hold Wemedoo, its directors, officers, employees and agents harmless from any and all demands, losses, liability, claims or expenses (including attorneys' fees) made against Wemedoo by any third party due to or arising out of or in connection with the Client's breach of any obligation of the Data Protection Law or this DPA.

In case of any conflict, this DPA shall take precedence over the regulations of the Agreement. Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

Upon the incorporation of this DPA into the Agreement, the parties indicated in Section 10 below (Parties to this DPA) are agreeing to the Standard Contractual Clauses (where and as applicable) and all appendixes attached thereto. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Annex, the Standard Contractual Clauses shall prevail, provided however: (a) Controller may exercise its right of audit under clause 8.9(c) and (d) of the Standard Contractual Clauses, and subject to the requirements of section 6 of this DPA; and (b) Processor may appoint sub-Processors as set out, and subject to the requirements of, section 4 and section 7 of this DPA.

The terms of this DPA are not publicly known and constitute confidential information. Controller may only disclose the terms of this DPA to a data subject or a Regulator to the extent required by law or regulatory authority. Controller shall take reasonable steps to ensure that Regulators do not make the terms of this DPA public, including by marking any copies as "Confidential", requesting return of any copies, and requesting prior notice and consultation before any public disclosure.

10. Parties to this DPA

This DPA is an amendment to and forms part of the Agreement. Upon the incorporation of this DPA into the Agreement, Controller and Wemedoo, who are each a party to the Agreement are also each a party to this DPA.

The legal entity agreeing to this DPA as Controller represents that it is authorized to agree to and enter into this DPA for and is agreeing to this DPA solely on behalf of, the Controller.

APPENDIX

ANNEX I

A. LIST OF PARTIES

As defined in the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of data subjects to which the DPA and the Clauses apply are different for each Tool provided by the Processor.

A. oomnia

Client information, Client's employees, contractors, agents, clients, and all other personnel involved in the conduction of the clinical trial (such as, for instance, doctors, medical workers, data managers, etc.). Regarding the personal data contained in the Clinical Trial Content (information about patients and similar), Wemedoo receives them from the Client in a pseudonymized form.

B. eConsent

Client information, Client's employees, contractors, agents, clients, and all other personnel involved in the conduction of the clinical trial (such as, for instance, doctors, medical workers, data managers, etc.), as well as Client's patients participating in the clinical trial.

C. ePRO

Client information (indirectly processed), Client's patients participating in the clinical trial.

Categories of personal data transferred

Categories of personal data to which the DPA and the Clauses apply are different for each Tool provided by the Processor.

Personal data	oomnia	eConsent	ePRO
Client employee's title (Mr/ Ms)	X		
Client employee's system user role	X	X	X
Client employee's first name	X	X	X
Client employee's last name	X	X	X
Client employee's username	X		
Client employee's e-mail address	X	X	X
Client employee's password	X	X	X
Client employee's address (country, city, street address, postal code)	X	X	X
Client employee's phone number	X		
Client employee's mobile number	X		
Client employee's fax	X		
Client employee's organization name	X	X	X
Client employee's position within the organization	X		
Client employee's clinical trials in which they are taking part	X	X	X
Client employee's roles within the trial organization	X	X	X

Client employee's system roles permissions	X	X	X
Client's Organization Name	X	X	X
Client's Organization Type	X	X	X
Client's Organization Full Address (Country, City, Street Address, Postal Code)	X		
Client's Organization Phone Number	X		
Client's Organization Time Zone	X		
Patient's identifier type for the clinical study (screening or participant ID)	X	X	X
Patient identifier number (screening or participant ID)	X	X	X
Patient's e-mail address		X	X
Patient's first name		X	X
Patient's last name		X	X
Patient's phone number		X	X
Patient's full address (country, city, street address, postal code)		X	X
Patient's language		X	X
Patient's signature (this is a digital signature created by entering password or a system generated one time token or 6-digit code)		X	
Patient's one-time code number sent for		X	X

two-factor authentication (valid for 3 to 5 minutes)			
Patient's health information provided for the purpose of a clinical trial conducted by the client	X	X	X
Information provided by the client's patients in the responses to the questionnaire for the purpose of a clinical trial conducted by the Client such as: name and surname, biometric data, photographs, or other data the patient decides to share with the client through the questionnaire			X
Patient's date of birth	X	X	X

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

oomnia:

The parties do not anticipate the transfer of special categories of data. Parties shall NOT disclose to each other any Personal data falling into special category of Personal Data as specified in the Data Protection Law. Namely, all the sensitive data provided by the Client is in an anonymized form. Also, the Client shall not use the Services in a way that would demand or motivate Data Subjects to provide such Personal Data.

eConsent:

The parties anticipate the transfer of Personal data falling into a special category of Personal Data as specified in the Data Protection Law. Namely, it is possible for the Client's patients to use the Questions and Answers section of the eConsent tool where they can voluntarily provide sensitive data, such as information about a person's health.

Given that the Processor's Service entails aiding the Client in executing clinical trials, it is inevitable that personal health information becomes accessible to the Processor. However, the Processor is granted this access solely for the purpose of maintaining the IT systems that support the Tools, and their processing will be reduced to a minimum since the Processor has no other interests in relation to this sensitive data. Adequate protection has also been established in accordance with Wemedoo's Rulebook on technical organizational measures and Annex 2 of this DPA.

ePRO:

The parties anticipate the transfer of Personal data falling into a special category of Personal Data as specified in the Data Protection Law. Namely, sensitive data will be transferred to the Processor via the ePRO tool in a structured and unified way collecting data on the health status, including the biometric data of participants in the clinical study through standardized forms.

Given that the Processor's Service entails aiding the Client in executing clinical trials, it is inevitable that personal health and/or biometric information becomes accessible to the Processor. However, the Processor is granted this access solely for the purpose of maintaining the IT systems that support the Tools, and their processing will be reduced to a minimum since the Processor has no other interests in relation to this sensitive data. Adequate protection has also been established in accordance with Wemedoo's Rulebook on technical organizational measures and Annex 2 of this DPA.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The data is transferred on a continuous basis.

Nature of the processing

The subject-matter of processing of Personal Data by Wemedoo is the provision of the Services to the Client via the Tool(s) that involves the processing of Personal Data. Personal Data will be subject to those processing activities as may be specified in the Agreement. The processing activities are collection, structuring, storage, retrieval, erasure, and destruction.

Purpose(s) of the data transfer and further processing

Personal Data will be processed for purposes of providing the Services set out via the Tool(s), as further instructed by Client in its use of the Services, and otherwise agreed to in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data will be processed for the duration of the Agreement.

For transfers to sub-processors, also specify subject matter, nature and duration of the processing

Wemedoo has concluded Data Processing Agreement with an affiliated company, the subprocessor Wemedoo Technologies doo, incorporated in accordance with the laws of the Republic of Serbia, CIN: 21787108, TIN: 113004928, with the registered seat at Tadije Sondermajera 3, Novi Beograd, Belgrade, Serbia, dated 19 July 2023. The nature of the processing is limited to the data processing activities related to the intercompany Master Service Agreement dated 01 July 2022, and the subject matter of transfer is provision of the services. Regarding the duration of processing, it shall be conducted as long as the Master Service Agreement is in force.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Wemedoo currently applies the security practices described in this Annex II. Wemedoo may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

The Processor implemented the following technical and organizational security measures to maximize protection of Personal data:

A. Access control to premises, computers, and technical equipment

- Business equipment for work may be used solely for business purposes when an employee is working remotely.
- In order to access computers and emails, employees are obliged to use passwords that must fulfill the following conditions: (i) has at least 8 characters; (ii) are not based on user's data (name, surname, date of birth, age, phone number, etc.); (iii) are easy to memorize; (iv) are not made from one word, i.e. are resistant to dictionary attacks.
- If an employee leaves the computer unattended, he/she is obliged to disable access to the computer, i.e., to lock the computer. After working hours, an employee is obliged to lock or shut down the computer and to clear the table from all documentation that contains personal information.
- Employees do not have access to personal data in absence of authorized personnel within Wemedoo who are allowed to process personal data.
- Wemedoo enters into separate non-disclosure agreements with every employee who has or may have access to personal data.
- Wemedoo implemented organizational measures such as 4-eye-principle and clear desk principle.
- Access rights hierarchy to areas and electronic storage locations are in place.

B. Access control to software and computer systems during personal data processing

- Software kept inside of business premises of Wemedoo is protected in such a manner that only authorized persons in accordance with appropriate service agreements have permission to access them.
- Repair, alteration and/or updates of computer systems must previously be approved by authorized person within Wemedoo and can be made only by authorized services and organizations and/or individuals who have concluded appropriate agreements with Wemedoo.
- Software used in computer informational system, and which are being received on data transmission media or via telecommunication channels, are being examined prior to their use in order to inspect whether they contain any computer viruses.
- First-time login procedure: User is forced to change password directly at first login.
- Website of Wemedoo runs on secured https protocol.
- Wemedoo performs vulnerability scanning and assessments on applications and infrastructure used to Process Personal Data.
- Wemedoo secures its computer networks using multiple layers of access controls to protect against unauthorized access.

- Wemedoo identifies computer systems and applications that warrant security event monitoring and logging, and reasonably maintains and analyzes log files.
- Wemedoo use up-to-date, industry standard, commercial virus/malware scanning software that identifies malicious code on all of its systems that Process Personal Data.
- Full backups are performed at minimum on daily basis, and outsourcing/copies of full backups are placed in different fire protection zone.

C. Receipt and transfer of personal data

- Personal data can be transferred by informational, telecommunication and other means only if appropriate measures and procedures for the prevention of unauthorized destruction, alteration, loss, access, processing, use and transfer of personal data are previously set in place.
- Personal data can be transferred only to users who previously deliver the evidence of the existence of appropriate legal ground, or based on the request, i.e. the consent of the data subject. Legal ground i.e. consent of data subject must be provided to Wemedoo in writing.
- All backups of personal data are encrypted on backup media.
- Each processing activity of personal data must be recorded and kept in an appropriate database, which contains information on Wemedoo acting as a data controller or data processor, data subjects, categories of personal data, subjects whom personal data are or will be shared with, international data transfer, if such transfer is made, the time period after which the data are being erased, as well as the general description of organizational and technical measures implemented by Wemedoo.
- Wemedoo uses the appropriate firewall and encryption technologies to protect the gateways and pipelines through which the data travels.
- Wemedoo monitors the completeness and correctness of the transfer of data via SSL (end-to-end check).
- Wemedoo has implemented procedures for safe disposal / destruction of Personal Data.

D. Personal data processing arising from sub-processing agreement

In case any activities related to personal data processing need to be delegated to a sub-processor, Wemedoo enters into a written agreement with the sub-processor which stipulates the mutual rights and obligations of Wemedoo and sub-processor. The agreement stipulates the requirements and measures securing the protection of personal data by the sub-processor.
Sub-processors which have concluded agreements with Wemedoo comply with legal requirements in terms of technical and organizational measures for personal data protection, in accordance with this DPA.
Sub-processors which have entered into agreements with Wemedoo are obliged to destroy or return personal data to Wemedoo after the processing of such data.

Wemedoo is using servers and cloud infrastructure of Microsoft Azure SQL Database.

Information about security of Microsoft Azure SQL Database:

a) Information about security of Microsoft Azure SQL Database https://docs.microsoft.com/en-us/azure/azure-sql/database/security-overview?view=azuresql
b) Information about physical security of Microsoft Azure SQL Database centres: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security
c) Information about GDPR compliance of Microsoft Azure SQL Database: https://azure.microsoft.com/en-us/blog/protecting-privacy-in-microsoft-azure-gdpr-azure-policy-updates/

APPENDIX III

This Appendix III applies in cases where the Personal Data are exported from Switzerland.

The respectively applicable set of Standard Contractual Clauses applies mutatis mutandis to data exports by WEMEDOO AG out of Switzerland.

The Standard Contractual Clauses (the SCC EU or SCCs) shall be deemed to be amended as follows:

- References to a "member state" or to the "EU" in the SCCs shall be deemed to include Switzerland.
- References to the GDPR should be understood as references to the Switzerland Data Protection Act insofar as the data transfers are subject to the Switzerland Data Protection Act
- Competent supervisory authority in Annex I.C under Clause 13: FDPIC is supervisory authority if the personal data transfer is governed by the Switzerland Data Protection Act.
- Applicable law for contractual claims under Clause 17: Swiss Law
- Place of jurisdiction for actions between the parties pursuant to Clause 18 b: Courts of Switzerland

Where an international transfer of personal data is subject to any law that protects legal entities as data subjects, the Parties agree that the SCC will apply to data relating to legal entities as well.

None of these amendments will have the effect or be construed to amend the SCCs in relation to the processing of personal data as it is subject to the GDPR.

APPENDIX IV

This Appendix IV ensures alignment with US Data Protection Laws and prevails over any conflicting provisions in the main body of the DPA regarding the processing of personal data under US laws. For the avoidance of doubt, the terms or conditions set forth in the DPA that are not otherwise addressed herein shall remain in full force and effect.

1. Scope of Processing and Compliance with US Data Protection Laws

a) This Appendix IV applies to all processing activities involving US Personal Data, as defined under applicable US Data Protection Laws, that Wemedoo processes on behalf of the Controller.

b) The Processor shall:
   i. adhere to the applicable US Data Protection Laws;
   ii. keep itself updated on legislative changes, with reasonable effort to align this Appendix IV with any updates or changes in US Data Protection Laws;
   iii. Processor shall notify the Controller promptly upon becoming aware of any legislative changes that may require an amendment to this Appendix;
   iv. ensure compliance with applicable data protection principles, including data minimization, purpose limitation, and transparency.

c) Each party acknowledges and agrees that the disclosure of US Personal Data to the other does not constitute and is not the intent of either party for such disclosure to constitute, a sale or sharing of US Personal Data.

d) Wemedoo shall:
   i. not collect, retain, use, or disclose US Personal Data for any purpose (including for any commercial purpose) other than for the specific purpose of performing the Services, unless otherwise required by law;
   ii. not sell or share US Personal Data, except as necessary to satisfy its obligations under the DPA;
   iii. not collect, retain, use, or disclose US Personal Data outside the direct business relationship between Wemedoo and Controller, unless expressly permitted by law;
   iv. not combine US Personal Data that the Wemedoo receives from, or on behalf of Controller with US Personal Data that Wemedoo receives from, or on behalf of, another party, or collects from its own interaction with a Data Subject, except to the extent reasonably necessary to conduct the Services and as expressly permitted by law;
   v. cease any unauthorized processing of US Personal Data at Controller's reasonable request and grant Controller authorization to assess and remediate any such unauthorized processing.

e) This DPA serves as Wemedoo's certification, to the extent required by CCPA or any other applicable Data Protection Law, that Wemedoo understands and will comply with the limitations on the processing of US Personal Data set forth in the Documented Instructions.

f) The parties further acknowledge and agree that Wemedoo shall process US Personal Data only for the specific "business purpose" of performing the Services set forth in the DPA, and that no valuable consideration is being exchanged for the disclosure of US Personal Data itself.

g) Wemedoo shall not engage in profiling, targeted advertising, or any form of behavioral analytics involving US Personal Data, except as expressly permitted by law or as reasonably necessary to conduct the Services.

2. Data Transfers and Sub-Processing

a) Wemedoo shall not transfer or otherwise disclose US Personal Data outside the United States without prior written consent from the Controller. If such transfers occur, Wemedoo shall ensure compliance with US Data Protection Laws.

b) The Processor may engage sub-Processors to support service delivery. However:

   i. a list of approved sub-Processors must be maintained and disclosed to the Controller;
   ii. the Controller must be notified in writing at least 30 days before engaging new sub-Processors;
   iii. the Controller reserves the right to object to any new sub-Processor on reasonable grounds; and
   iv. Wemedoo must using reasonable measures ensure all sub-Processors adhere to obligations consistent with this Appendix IV.

3. Security of processing and data breaches

a) Wemedoo shall implement appropriate technical and organizational security measures aligned with industry standards, ensuring:

   i. encryption and pseudonymization of Personal Data;
   ii. access control mechanisms limiting access to authorized personnel;
   iii. incident monitoring systems to detect security threats;
   iv. regular audits of security policies and infrastructure.

b) In the event of a Personal Data Breach, Wemedoo shall:

   i. notify the Controller without undue delay, but no later than 72 hours after becoming aware of the breach;
   ii. provide all necessary details, including:
      I. the nature and scope of the breach;

II. impacted data subjects and categories of Personal Data;
III. corrective measures taken to mitigate risks.

4. Data subject rights

a) Wemedoo shall:
   i. assist the Controller in fulfilling Data Subject Rights under US Data Protection Laws;
   ii. facilitate requests for access, correction, deletion, opt-out, and portability;
   iii. redirect any direct Data Subject Requests to the Controller within a reasonable timeframe and shall not respond to such requests directly unless authorised by the Controller.

5. CCPA Compliance and Audits

a) Wemedoo shall:
   i. maintain compliance with the CCPA and CPRA;
   ii. notify the Controller if it determines that it can no longer meet its obligations under the CCPA;
b) the Controller may audit Wemedoo to ensure CCPA compliance;
c) if unauthorized use of US Personal Data is identified, the Controller may take reasonable and appropriate steps to remediate non-compliance;
d) the parties confirm that the disclosure of US Personal Data under this DPA does not constitute a sale under the CCPA and CPRA.