Supplemental Agreement on Data Processing on behalf of a Controller

between

_____

(“**Controller**”)

and

Brainlab Ltd., Regus House, 1010 Cambourne Business Park, Cambourne, Cambridge, CB36DP, United Kingdom
(“**Processor**”, together the “**Parties**”)

Preamble

This agreement applies to the activities provided by the Processor regarding the installation of hard- and software, maintenance, repair, training, remote access, trouble shooting and any other service work for the Processor’s products which support Controller to provide healthcare, and in the course of which employees of Processor or third parties commissioned by Processor might get in contact with Personal Data of Controller. The underlying agreements regarding these activities or services shall in the following be referred to as the Master Agreement.

This Supplemental Agreement is concluded in accordance with the Master Agreement and shall align to the term of the Master Agreement.

1. Definitions

In this agreement, the following terms shall have the following meanings:

"**Adequate Country**" shall mean any country outside of the EEA that is recognized by the European Commission as providing an adequate level of privacy protection by reason of its domestic law or of the international commitments it has entered into;

“**GDPR**” shall mean 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);

“**Instruction**” shall mean written instructions by Controller on the specific handling of Personal Data (e.g. anonymisation, blocking, deletion, handing over) by Processor with regard to data protection.

“**Personal Data**”, “**Controller**”, “**Processor**”, “**process/processing**”, “**data subject**”, “**technical and organisational measures**”, “**supervisory authority**” or “**processing on behalf of a Controller”** shall be interpreted in accordance with the GDPR.

2. Subject matter and responsibility

Processor processes Personal Data on behalf of Controller. Subject matter of the commissioning are activities as specified in the Master Agreement and the schedules annexed to the Master Agreement, in particular the specification of services. Within the scope of this Supplemental Agreement, Controller shall be solely responsible for

compliance with the statutory provisions on data protection, in particular the lawfulness of the transfer of data to Processor and the processing of the data through Processor.

3. Specification of the commissioning, limited territoriality

3.1 Purpose, type and extent of the commissioned collection, processing and/or use of Personal Data are described in the Master Agreement to which insofar explicit reference is made.

3.2 The type of categories of the collected and/or used Personal Data as well as the category of data subjects who are subject to the handling of Personal Data under this commissioning are further described in Annex 1 and/or the Master Agreement to which insofar explicit reference is made.

4. Controller's right to issue instructions

4.1 Within the scope of the specifications set forth in this Supplemental Agreement, Controller reserves the right to issue Instructions concerning the type, extent and procedure of data processing which it may specify by issuing Individual Instructions. Changes of the subject matter of processing and procedures shall be jointly agreed upon and shall be documented.

4.2 Processor will inform Controller of any Instruction that it deems to be in violation of data protection requirements. Processor may then postpone the execution of the relevant Instruction until it is confirmed or changed by Controller.

5. Obligations of Processor

5.1 Basically, Processor shall, unless otherwise permitted by law or otherwise (e.g. data subject's consent), collect, process or use data only as commissioned by Controller and in compliance with the Instructions of Controller but, in particular, not for its own purposes. Processor will correct, delete, rectify or block the data processed on behalf of Controller only as instructed by Controller. If a data subject contacts Processor with a request for correction or deletion of its data, Processor shall forward the request to Controller.

5.2 Processor shall also be entitled to use certain data which it receives in the course of providing product support in a form that will not allow the respective Processor personnel to re-identify any natural person (e.g. a physician, hospital staff or patient). Such use occurs for the purposes of (i) fulfilling legal obligations (e.g. product monitoring and reporting obligations), or (ii) exercising other legitimate interests and lawful purposes of Processor and Controller, in particular those to improve the quality and functionality of Processor's products by using selected support data (e.g. de-identified CT or MRT images) to *i.a.* test new releases of the products.

5.3 Processing takes place on the Instructions from the Controller only, unless the Processor is required to do so by European Union or Member State law to which the Processor is subject to; in such a case, the Processor shall inform the Controller of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest (cf., Art. 28 para. 3 lit. a GDPR).

5.4 Unless prohibited by applicable law or a legally-binding request of an authority, Processor shall promptly notify Controller of any request by public authorities, data protection supervisory authority or law enforcement authority for access to or seizure of Personal Data of the Controller as provided hereunder.

5.5 Before granting access to Personal Data, Processor will oblige persons employed in processing Personal Data on data secrecy and confidentiality and familiarize them with the provisions as set forth in the data protection obligations as applicable to Processor.

Where necessary, this shall include obligating the relevant personnel on professional secrecy (if any, including derivative obligations, for example when processing data originating from hospitals or medical doctors) or the telecommunication secrecy if and to the extent that respective services have been agreed upon in the Master Agreement. If required by professional law and professional conduct rules, Controller shall take all necessary measures or coordinate them with its customers and inform and instruct the Processor accordingly.

5.6 Insofar as required by statutory law, Processor will appoint a data protection officer and shall make its contact details available to Controller during the term of this Agreement.

5.7 Processor will without undue delay notify Controller of violations of Instructions or of provisions for the protection of Controller's Personal Data by Processor or a person employed by Processor.

If Personal Data have been lost, unlawfully transferred or otherwise unlawfully disclosed to third parties according to Art. 33 and 34 of the GDPR, Controller shall be informed of such incidents without undue delay. Processor shall, in consultation with Controller, take appropriate measures to safeguard the data as well as to mitigate potentially adverse consequences for the data subjects.

Furthermore, Processor shall without undue delay inform Controller of serious disruptions of the normal course of operations, any suspicions of data protection violations or other irregularities in processing the data of Controller.

Processor acknowledges that Controller is obliged to document breaches of the protection of Personal Data and, if necessary, inform the supervisory authority, respectively the data subject, on such breach. If and insofar as it has come to such breaches, Processor will assist the Controller in accordance with Art. 28 para. 3 lit. f GDPR with compliance of its reporting obligations in a proper manner to allow for the Controller to timely perform its obligations hereunder. Processor will notify the breach to the Controller and provide at least the following information as far as Processor has the relevant information:

(a) description of the kind of breach, if possible the category and the approximate amount of data subjects and datasets involved,

(b) name and contact of a contact person for further information,

(c) description on the probable consequences of the breach,

(d) description of the taken measures in order to remedy or reduce the breach.

5.8 Processor will inform Controller of any monitoring activity of and measures taken by the supervisory authority with regard to the processing of Personal Data of Controller.

5.9 If Controller is obliged in accordance with applicable statutory data protection law to provide information on the collection, processing or use of data, Processor shall provide Controller with any and all respective information.

5.10 Processor shall monitor the compliance with obligations specified above during the execution of the commissioned data processing.

5.11 Processor shall maintain a written record of all categories of processing activities carried out on behalf of the Controller in accordance with Art. 30 para. 2 of the GDPR.

5.12 If applicable, Processor assists in accordance with Art. 28 para. 3 lit. f GDPR with the preparation of a data protection impact assessment pursuant to Art. 35 GDPR and, where appropriate, assists with the prior consultation of the supervisory authority pursuant to Art. 36 GDPR. On Controller's request, Processor shall disclose the required information and documents to Controller. The additional costs incurred by these services are to be reimbursed to the Processor.

5.13 The Processor shall implement appropriate measures in respect of data misuse, data loss and recoverability of data (e.g. by creating industry standard backups), as far as this is agreed in the Master Agreement.

6. Security of Processing

6.1 Within its scope of responsibility, Processor will set up its internal organization in accordance with all applicable data protection and data security requirements. Processor shall take, maintain and control technical and organisational measures to ensure reasonable protection of Controller's data against misuse and loss in accordance with the requirements according to applicable laws.

6.2 Processor takes all appropriate technical and organisational measures that comply with the requirements of Art. 32 GDPR, in order to ensure a level of security appropriate to the risk and assist the Controller in ensuring compliance with the obligations pursuant to Art. 32 GDPR (Art. 28 para. 3 lit. c, f GDPR).

6.3 In this context, the Processor shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. This includes appropriate measures on e.g. entrance control, user control, access control, transmission control, input control, job control, availability control as well as separation by purpose and, inter alia as appropriate, the pseudonymization and encryption of Personal Data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.4 Annex 2 contains a description and specification of the required technical and organisational measures Processor will implement hereunder. These may be complemented by further related documentation provided by the Processor during or in the course of providing the services.

6.5 Technical and organisational measures are subject to technical progress and development. The Processor may implement adequate alternative measures. These must not, however, fall short of the level of security provided by the specified measures. Any material changes must be documented.

6.6 Processor assists the Controller in accordance with Art. 28 para. 3 lit. e GDPR by appropriate technical and organisational measures, insofar as this is possible and reasonable, for the fulfilment of Controller's obligation pursuant to Chapter III of the GDPR towards data subjects, e.g. the information to and access of the data subjects, rectification and erasure of data, restriction of processing or the right to data portability and right to object. The additional costs incurred by this assistance are to be reimbursed to the Processor.

7. Remote and Support access

7.1 The following supplementary regulations apply to the performance of remote and support access if and to the extent that the processing activities concern special categories of Personal Data or Controller is subject to professional secrecy.

7.2 Remote access shall only be carried out with the consent of an authorised person of the Controller, if and to the extent that access to Personal Data cannot be excluded.

7.3 The employees of the Processor shall use appropriate identification and encryption methods.

7.4 Remote access work shall be documented and recorded. The Controller is entitled to inspect inspection and maintenance work before, during and after execution while in doing so it shall follow the provisions as set forth under Section 9. In case of remote access, the Controller is entitled - as far as technically possible and feasible with regards to the nature of the services provided - to follow these from a control screen and to cancel them at any time.

7.5 Remote access to the relevant systems shall be performed on a need-to-know basis only.

7.6 Fault analysis that requires access to Personal Data, requires the prior consent of an authorised person of the Controller. If copied for such purposes, the Processor shall either modify it so that Processor cannot identify from it a natural person anymore, or delete these copies after correction of the error, except if storage of the (unmodified) data is necessary for other purposes (e.g. documentation of the correctness of the performed activities). Personal Data may only be used for the purpose of fault analysis and may furthermore not be copied to mobile storage media (PDAs, USB memory sticks or similar devices) without appropriate encryption. Section 5.2 remains unaffected.

7.7 In individual cases, Processor may perform fault analysis work without obtaining prior consent of an authorised person of the Controller if it will be necessary to perform the agreed services (in particular repair work). Controller herewith declares its general consent for Processor to perform such activities accordingly.

7.8 Remote access and all activities required in this context, in particular activities such as deletion, data transfer or fault analysis, shall be carried out taking into account technical and organisational measures for the protection of Personal Data.

8. Rights and obligations of Controller

8.1 Controller and Processor shall each be responsible for compliance with the respective statutory data protection law as it applies to the one or the other with regard to the Personal Data that are to be processed hereunder.

8.2 Controller shall specify the measures for returning the provided data media and/or deletion of recorded data after the termination of the commissioning by way of entering into a contract. If no specifications are issued, data shall be handed over to Controller or destroyed. Insofar as data are deleted in accordance with particular specifications, Processor shall confirm such deletion to Controller specifying the date on which such deletion has been effected. The return or deletion of stored data is subject to legal or regulatory retention obligations and permits applicable to the Processor. Section 5.2 remains unaffected.

9. Audit Rights

9.1 On request of the Controller the Processor shall provide the Controller with evidence of the implementation of the technical and organisational measures and the other obligations stated in Art. 28 GDPR.

9.2 Controller may carry out job control in consultation with the Processor, or appoint auditors to do so before the start of data processing and in a reasonable manner throughout the term of the Master Agreement. The Processor may comply with such requests by providing Controller at any time before the start of and throughout the term of the processing with respective self-audits, up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department, data protection or quality auditors) or suitable certification by way of an IT security or data protection audit.

9.3 If the Controller has reasonable doubts regarding the self-audit or evaluation provided by the Processor and provides the Processor with an explanation of such doubts, Controller

shall be entitled, at its own expenses, to carry out a reasonable check on the Processor's business premises in order and insofar as to verify the implementation of the technical and organisational measures and the other obligations stated in Art. 28 GDPR. Such audit shall be announced at least two weeks in advance, only be performed during regular business hours and shall not disturb internal operations. Controller shall remunerate any additional costs incurred by Processor due to such audit.

9.4 Upon Controller's written request, Processor shall provide Controller within a reasonable period of time any information and make the documentation available as necessary for the audit.

10. Sub-Processors

10.1 Processor shall be entitled to use subcontractors and other companies for fulfilling its contractual obligations.

10.2 Processor shall ensure by entering into agreements with sub-processors to impose at least substantially the same obligations on sub-processors which Processor has assumed according to this Supplemental Agreement prior to sub-processor being granted access to Controller's Personal Data during its performance. If the sub-processor provides the agreed service outside the EU/EEA and an Adequate Country, Processor shall comply with EU Data Protection Regulations by taking appropriate measures.

10.3 Upon request, Processor shall provide a list of sub-processors involved in the data processing activities hereunder. Processor shall inform the Controller of any intended changes concerning the addition or replacement of other sub-processors, thereby giving the Controller the opportunity to object to such changes, whereas Controller has to present reasonable grounds for such an objection. If Controller still does not approve of a new sub-processor, then Controller and/or Processor may terminate the affected parts of the services without penalty by providing, before the end of any applicable notice period, written notice of termination.

10.4 Controller shall be entitled to audit Processor's sub-processors in accordance with Section 9 above and upon prior consultation and agreement with Processor to that effect, whereas Controller herewith commissions Processor with executing such audits on Controller's behalf and agrees that such audit may only be executed by Processor and may also be satisfied by presenting up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department, data protection or quality auditors) or suitable certification by way of an IT security or data protection audit. Controller acknowledges that it may have to execute one or more confidentiality agreements with Processor and/or its sub-processor before receiving respective documents and information.

10.5 Approval requirements for subcontracting shall not apply in cases where Processor subcontracts ancillary services to third parties; such ancillary services shall include, but not be limited to mail, shipping and receiving services and caretaking services.

11. Territory

11.1 As a general rule, the processing shall occur in a member state of the European Union, in a country of the European Economic Area or in an Adequate Country (for the purpose of this Schedule including the USA, if a Privacy Shield certificate exists). Processing activities in another country ("**Third Country**") shall be allowed if the applicable requirements for international transfer of Personal Data according to Art. 44 ff. GDPR are complied with.

11.2 If and to the extent that (i) Controller and Processor are located within the Economic European Area ("**EEA**") while the sub-processor is located in a Third Country and (ii)

Processor will enter into agreements with sub-processors based on the EU Standard Contractual Clauses for Processors ("**SCC**"), Controller herewith authorizes Processor to enter into such sub-processing agreements with sub-processors – as far as possible for Processor - also in the name and on behalf of Controller. Upon request, Processor shall inform Controller of the existence and status of such Standard Contractual Clauses Agreements entered into under the above circumstances. It is at the discretion of the Processor whether such contracts are concluded.

12. Liability

12.1 Controller shall defend and hold harmless Processor from any third party claim or other losses or liabilities arising from (i) the Controller's breach of its obligations hereunder and/or other violations of applicable data protection laws of Controller, or (ii) Processor's breach of applicable data protection laws if such breach has been caused by Processor's performance of the provisions in this Supplemental Agreement or Controller's Instruction. Such obligation shall not exist, where Controller is not responsible for such third party claim or other losses or liabilities. Art. 82 (5) GDPR shall remain unaffected.

12.2 In any case, to the extent the Master Agreement provides for a limitation or exclusion of Processor's liability or indemnification obligations, those limits or exclusions shall apply accordingly for claims asserted against Processor hereunder.

12.3 The provisions in the Master Agreement addressing liability or indemnification obligations shall remain unaffected.

13. Confidentiality

The Parties shall undertake to treat as confidential any knowledge of operational and trade secrets acquired within the scope of the contractual relationship. This shall continue to apply beyond the term of individual orders and/or the business relationship.

14. Duty to inform, written form requirement, choice of law

14.1 If there is a risk that Personal Data of Controller becomes the subject of attachment or seizure, insolvency or settlement proceedings or other incidents or third party measures at Processor, Processor shall immediately notify Controller thereof. Processor will inform all persons responsible in this context, that exclusive authority to dispose and ownership with regard to the data lies with Controller.

14.2 Modifications and amendments of this Supplemental Agreement are only effective if made in writing and if explicit reference is made to the fact that this Supplemental Agreement shall thereby be modified or amended. This shall apply accordingly to a deviation from this form requirement.

14.3 This Supplemental Agreement and all legal disputes arising in connection with its taking effect or its performance shall be exclusively subject to German law excluding the Vienna Convention of the United Nations Convention on Contracts for the International Sale of Goods of April 11, 1980 (CISG). Place of jurisdiction for any disputes between the Parties in connection with this Supplemental Agreement shall be the regional court of Munich I.

For Processor:	**For Controller:**
[*Name*]	[*Name]*
[*Position*]	[*Position*]
[*Place, Date*]	[*Place, Date*]
_____	_____

<u>Annex 1</u>: **Type of data categories and categories of data subjects within the scope of the collection, processing and/or use of Personal Data**

1. Type of collected and/or used Personal Data

- Personal master data (e.g. first and last name, date of birth, gender, patient ID)
- Contact details (e.g. telephone, email)
- Contract master data (e.g. contractual relationship, interest in products or contracts)
- Customer history
- Billing and payment data (e.g. bank account number)
- Planning and management data (e.g. customer infrastructure information)
- Rating data (from third parties, e.g. rating agencies, or from public directories)
- Medical information and images of patients

2. Categories of data subjects who are subjected to the handling of Personal Data

- Customers
- Prospects
- Subscribers
- Patients of Customers

Annex 2: **Security of the processing**

This Annex describes the TOMs and procedures that Processor shall, as a minimum, maintain to protect the security of Personal Data created, collected, received, or otherwise obtained and ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

Technical and Organizational Measures

I. Confidentiality, Art. 32 para. 1 lit. b) GDPR

1. Physical Access Control

Measures appropriate for preventing unauthorized persons from accessing data processing systems for processing or using personal data.

- ☒ Definition of a restricted group of persons with access rights
- ☒ Safety locks
- ☒ Manual locking system (e.g. lockable room, cabinet) – applicable specifically for Home Office
- ☒ Smartcard/transponder locking system
- ☒ Video monitoring of entrances

2. Logical Access Control

Measures appropriate for preventing unauthorized persons from using data processing systems.

- ☒ Functional and/or time-limited assignment of user authorizations
- ☒ Password policy including regulations regarding password length, assignment and changes
- ☒ Authentication with user name / password
- ☒ Use of intrusion detection systems and intrusion prevention systems
- ☒ Use of antivirus software
- ☒ Use of a hardware firewall
- ☒ Use of e-mail spam filters
- ☒ Creation of user profiles
- ☒ Assignment of user profiles to IT systems
- ☒ Use of VPN technology
- ☒ Use of central smartphone administration software (e.g. for external deletion of data)
- ☒ Use of a software firewall
- ☒ Laptop hard disc encryption
- ☒ Additional login system for different applications

3. Data Access Control

Measures to ensure that persons authorized to use a data processing system have only access to data within the scope of their access rights and to ensure that personal data cannot be read, copied, changed or deleted by unauthorized persons during processing and use and after saving.

- ☒ Definition of access rights
- ☒ Administration of rights by the system administrator
- ☒ Restrictive allocation of administrator permissions
- ☒ Safe storage of data media
- ☒ Physical deletion of data media before reuse
- ☒ Logging of accesses to different applications
- ☒ Logging of data transmissions
- ☒ Defined procedures for granting, controlling and withdrawing permissions
- ☒ Required password identification
- ☒ Secure destruction of data carriers

4. Separation Control

Measures to ensure that data collected for different purposes can be processed separately.

- ☒ Physically separated saving to dedicated systems or data media
- ☒ (Software-based) logical multi-tenancy
- ☒ Creation of an access rights policy
- ☒ Separation of output and test system

II. Pseudonymisation and encryption, Art. 32 para. 1 lit. a) GDPR

Measures for the pseudonymisation and encryption of personal data (if not already mentioned in section I.).

- ☒ Use of pseudonymisation and anonymisation techniques, i.a. in the field of R&D
- ☒ Standard encryption of particularly sensitive data (at rest) in individual services
- ☒ Existence of rules and regulations for data encryption

III. Integrity, Art. 32 para. 1 lit. b) GDPR

1. Data Transfer Control

Measures to ensure that personal data cannot be read, copied, changed or deleted by unauthorized persons during electronic transfer, transport and saving to carrier media and to allow checking and tracing to which places or bodies the transfer of personal data by data transfer devices is intended.

- ☒ Setup of dedicated lines or VPN tunnels
- ☒ A guideline exists with clear provisions what to do when data media go astray

☒ Staff training on data protection

☒ Laptop hard disk encryption

☒ Documentation of recipients of data

2. Data Entry Control

Measures to ensure that it can be checked and traced retrospectively whether and by whom personal data was entered into data processing systems or changed or removed.

☒ Assignment of rights for entry, changes and deletion of data based on an access right policy

☒ Recording of entry, changes and deletion of data, as far as enabled by the systems

IV. Availability and resilience, Art. 32 para. 1 lit. b) und c) GDPR

Availability Control

Measures ensuring that personal data is protected against accidental destruction or loss, including recovery measures in the event of physical or technical incidents.

☒ Uninterruptible power supply (UPS)

☒ Climate control in server rooms

☒ Fire and smoke detection equipment

☒ Appropriate fire extinguishing system in server rooms

☒ Backup & recovery policy

☒ Data recovery testing

☒ Existence of an emergency plan

☒ Storage of backup medium at a safe external location

☒ Use of firewalls and virus scanners

☒ Patch management

V. Process for regularly testing and evaluating, Art. 32 para. 1 lit. d) GDPR

1. Data Protection Management

Other measures, in particular organisational measures to protect personal data.

☒ Description of applicable data protection regulations in binding guidelines and instructions

☒ Regular testing of data protection measures and existing regulations

☒ Obtaining up-to-date information on IT security and IT vulnerabilities

☒ If necessary, involvement of the data protection officer in relevant new data processing procedures

2. Incident Response Management

Other measures for managing data protection incidents.

☒ Policy for data protection and IT security incidents

☒ Business Continuity Management Processes

☒ Incident reporting process

3. Privacy by default, Art. 25 para. 2 DSGVO

Measures to ensure that pre-settings meet the interests of the data subjects (privacy by default).

☒ Implementation of data protection-friendly pre-settings

☒ Use of pseudo- or anonymisation of personal data, e. g. in the area of R&D

☒ Restriction of data collection

4. Order Control

Measures ensuring that personal data processed on behalf of others can only be processed according to the instructions of the client.

☒ Selection of the contractor involving diligence criteria (in particular with respect to data security)

☒ Preliminary check of the data processor, in particular prior evaluation of the documentation of the security measures taken by the contractor

☒ Documented instructions to the contractor (e.g. by a contractor data processing agreement)

☒ Obligation of the processor to oblige its staff to data confidentiality

☒ Contractor may have assigned a data protection officer

☒ Effective control rights agreed with the contractor

☒ Training of staff

☒ Records of processing activities