Data Processing Agreement

between

End User

and

University College London

1. Parties to this Agreement

(a) **END USER** an individual accessing the k-Plan software, a cloud-based software platform for planning therapeutic ultrasound treatments in the brain, pursuant to its agreement with Brainbox Ltd, a company registered with company number 07288205 of 8a Morgan Arcade, Cardiff, Wales, CF10 1AF (**You** or the **End User**); and

(b) **UNIVERSITY COLLEGE LONDON** a body corporate established by Royal Charter with company number RC000631 of Gower Street, London, WC1E 6BT (**UCL**).

2. Background

(a) The End User wishes to access the k-Plan software pursuant to entering into an agreement with Brainbox Ltd, a company registered with company number 07288205 of 8a Morgan Arcade, Cardiff, Wales, CF10 1AF (**Brainbox Agreement**).

(b) This Agreement establishes the terms and conditions under which UCL will process Personal Data supplied to it by the End User when accessing the k-Plan software. This Agreement contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR) for contracts between controllers and processors [and the General Data Protection Regulation ((EU) 2016/679)].

3. Terms of the Agreement

(a) This Agreement comprises these terms and conditions and the Schedules attached hereto.

(b) For clarity, the Schedules form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.

(c) The End User shall share the Personal Data with UCL by adding planning images to the k-Plan software and selecting to upload these to the k-Plan cloud servers for processing, and UCL shall process that Personal Data, only in accordance with the terms of this Agreement.

4. Term and termination

(a) This Agreement shall commence when the End User accepts the terms and conditions of this data processing agreement as part of the software installation and by selecting to evaluate a treatment plan using the k-Plan software.

(b) Without prejudice to any other right or remedy available to it, UCL may terminate this Agreement at any time for any reason with immediate effect by giving 28 days' written notice.

(c) Clause 4 (Term and termination), Clause 5 (Data protection arrangements) and Clause 6 (indemnity) shall survive the termination or expiry of this Agreement, as shall any other Clause which, by its nature, is intended to survive termination or expiry.

(d) Termination or expiry of this Agreement shall not affect any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of the agreement which existed at or before the date of termination or expiry.

5. Data protection

(a) The parties agree and acknowledge that the End User shall be the Data Controller of all Personal Data Processed by UCL in connection with this Agreement, and UCL shall be the Data Processor in respect of such Personal Data.

Obligations applicable to the Data Processor (UCL)

(b) UCL shall:

(i) comply with all applicable provisions of the Data Protection Legislation;

(ii) only process the Personal Data pursuant to Schedule 2 which describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the UCL may process the Personal Data supplied to it by the End User

(iii) Not used;

(iv) notify the End User immediately (and in any event within twenty-four (24) hours of becoming aware of the same) if it considers, in its opinion (acting reasonably) that there has been an infringement of Data Protection Legislation pursuant to this agreement;

(v) implement and maintain appropriate technical and organisational security measures, including the encryption of personal data in transit and at rest and in accordance with the particulars set out in Schedule 2, which are sufficient to comply with Data Protection Legislation;

(vi) where applicable, take all reasonable steps, including the provision of appropriate training in data protection and information security, to ensure the reliability, competence and integrity of any of the Personnel who shall have access to the Personal Data, ensure that each member of Personnel shall

have entered into appropriate contractually-binding confidentiality undertakings, and all times procure compliance by those persons with such obligations of confidentiality;

(vii) not transfer any Personal Data pursuant to this Agreement out of the United Kingdom / EEA / EU, other than directly to the Data Controller. The Data Controller shall notify UCL as and when further measures are required to comply with Data Transfers outside of the United Kingdom / EEA / EU and shall be responsible for issuing any further documentation to facilitate a Data Transfer.

(viii) notify the End User promptly (and in any event within forty-eight (48) hours) following its receipt of any Data Subject Request or Regulator Correspondence pursuant to this agreement and shall: (A) not disclose any Personal Data in response to any Data Subject Request or Regulator Correspondence without consulting with the End User; and (B) provide the End User with all reasonable co-operation and assistance required by the End User in relation to any such Data Subject Request or Regulator Correspondence;

(ix) notify the End User promptly upon becoming aware of any actual or suspected, threatened or 'near miss' Personal Data Breach, with sufficient information to allow the End User to meet any obligations under Data Protection Legislation to report or inform Data Subjects of the data breach, and: (A) implement any measures necessary to restore the security of compromised Personal Data; and (B) assist the Data Controller to make any notifications to the Regulator and affected Data Subjects;

(x) except to the extent permitted by Applicable EU Law, upon the End User's request and/or on the earlier of: (A) termination or expiry of this Agreement (as applicable); and/ or (B) the date on which the Personal Data Processed in connection with this Agreement is no longer relevant to, or necessary for, the Permitted Purpose, the UCL shall cease Processing all such Personal Data and return and/ or permanently and securely destroy, so that it is no longer retrievable (as directed in writing by the End User), all such Personal Data and all copies in its possession or control (including back up copies); and

(xi) use all reasonable endeavours, in accordance with Good Industry Practice, to assist the End User to comply with the obligations imposed on the End User by the Data Protection Legislation, including: (A) compliance with the Security Requirements; (B) obligations relating to notifications required by the Data Protection Legislation to the Regulator and/ or any relevant Data Subjects; and (C) undertaking any Data Protection Impact Assessments (and, where required by the Data Protection Legislation, consulting with the Regulator in respect of any such Data Protection Impact Assessments).

Obligations applicable to both UCL and the End User

(c) During the term of this Agreement each party acknowledges that it has obligations under applicable Data Protection Legislation including the following (for clarity, these obligations shall be without prejudice to the obligations applicable to the UCL set out at Clause 5(b) above):

(i) to make due notification (where required by applicable Data Protection Legislation) to the Regulator, including in relation to its use and Processing of the Personal Data and comply at all times with the Data Protection Legislation;

(ii) to ensure that all Personal Data disclosed or transferred to, or accessed by, the other party is accurate and up-to-date, as well as adequate, relevant and not excessive to enable each party to Process the Personal Data, as envisaged under this Agreement;

(iii) to ensure that appropriate operational and technical measures, including encryption implemented to the appropriate Current Standard, are in place to safeguard against any unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data and where requested provide to the other party evidence of its compliance with such requirement;

(iv) take reasonable steps to ensure the reliability of any personnel who have access to the Personal Data;

(v) hold the information contained in the Personal Data confidentially; and

(vi) not do anything which shall damage the reputation of the other party or that party's relationship with the Data Subjects.

(d) Notwithstanding anything in this Agreement to the contrary, this Clause 5 (Data Protection Arrangements) shall continue in full force and effect for so long as the End User is a Party to the Brainbox Agreement.

6. Indemnity

(a) The End User hereby indemnifies UCL against all costs, claims, liabilities and expenses (including reasonable legal expenses) incurred by UCL in connection with or as a result of any breach of this Agreement by the End User, its staff or agents.

7. Miscellaneous

(a) No variation of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

(b) A failure or delay by a party to exercise any right or remedy provided under this Agreement or by law shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under this agreement or by law shall prevent or restrict the further exercise of that or any other right or remedy.

(c) If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this Clause shall not affect the validity and enforceability of the rest of this Agreement.

(d) This Agreement constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

(e) Each party agrees that it shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement.

(f) Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.

(g) This Agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

(h) This Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.

(i) This agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with English law.

(j) Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this agreement or its subject matter or formation.

Schedule 1: Definitions and interpretation

1. Definitions

Applicable EU Law	means any law of the European Union (or the law of one of the Member States of the European Union) to which UCL is subject;
Commercially Sensitive Information	means information of a commercially sensitive nature relating to the UCL, its intellectual property rights or its business or which the UCL has indicated to the End User that, if disclosed by the End User, would cause UCL significant commercial disadvantage or material financial loss;
Confidential Information	any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and suppliers of UCL, including intellectual property rights, together with all information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential, including Commercially Sensitive Information;
Current Standard	means the current standards for encryption recommended by the Information Commissioner's Office, such as FIPS 140-2 (cryptographic modules, software and hardware) and FIPS 197;
Data Controller	has the meaning set out in the Data Protection Legislation;
Data Processor	has the meaning set out in the Data Protection Legislation;
Data Protection Impact Assessment	means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data, as required by Article 35 of the GDPR;
Data Protection Legislation	means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a party to this Agreement is subject, including: (a) the Data Protection Act 1998 and EC Directive 95/46/EC (up to and including 24 May 2018); and (b) the GDPR (from and including 25 May 2018); and/or (c) in the event that the UK leaves the European Union, all legislation enacted in the UK in respect of the protection of Personal Data;
Data Protection Particulars	means, in relation to the Processing under this Agreement: (a) the subject matter and duration of the Processing; (b) the nature and purpose of the Processing; (c) the type of Personal Data being Processed; and (d) the categories of Data Subjects, as set out in Schedule 2;
Data Subject Request	means an actual or purported subject access request or notice or complaint from (or on behalf of) a Data Subject exercising its rights under the Data Protection Legislation;
Data Subject	has the meaning given to it in the Data Protection Legislation;
Data Transfer Risk Assessment	means a risk assessment which set out details of the following: (a) the Personal Data that will be transferred; (b) the Restricted Country or Countries to which the Personal Data will be transferred;

	(c) the means by which the Data Processor will ensure an appropriate level of protection and appropriate safeguards in respect of the Personal Data that will be transferred to a Restricted Country so as to ensure the Data Processor's compliance with Data Protection Legislation; and (d) in providing and evaluating the risk assessment, the Data Processor shall ensure that it has regard to the Data Protection Legislation in connection with transfers of Personal Data to any Restricted Country;
Data Transfer	means transferring the Personal Data to, and/ or accessing the Personal Data from and/ or Processing the Personal Data within, a jurisdiction or territory that is a Restricted Country;
EIRs	means the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such regulations;
FOIA	means the Freedom of Information Act 2000, and any subordinate legislation made under the Act from time to time, together with any guidance and/or codes of practice issued by the Regulator or relevant government department in relation to such legislation;
GDPR	means 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 repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5.2016;
Good Industry Practice	means, at any time, the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of similar services to those being carried out under this Agreement, such supplier seeking to comply with its contractual obligations in full and complying with all applicable laws (including the Data Protection Legislation);
Information:	has the meaning given under section 84 of FOIA;
Permitted Purpose	means the purpose of the Processing as set out in more detail in the Data Protection Particulars;
Personal Data Breach	has the meaning set out in the Data Protection Legislation;
Personal Data	means any Personal Data (as defined in the Data Protection Legislation) processed by either Party in connection with this Agreement;
Personnel	means all persons engaged or employed from time to time by the Data Processor in connection with this Agreement, including employees, consultants, contractors and permitted agents;
Process or Processing	has the meaning set out in the Data Protection Legislation;
Regulator	means the UK Information Commissioner (including any successor or replacement);
Restricted Country	means a country, territory or jurisdiction outside of the European Economic Area which the EU Commission has not deemed to provide adequate protection in accordance with EC Directive 95/46/EC and/or Article 45(1) of the GDPR (as applicable);

Request for Information	means a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations;
Security Requirements	means the requirements regarding the security of the Personal Data, as set out in the Data Protection Legislation (including, in particular, the seventh data protection principle of the Data Protection Act 1998 and/ or the measures set out in Article 32(1) of the GDPR (taking due account of the matters described in Article 32(2) of the GDPR)) as applicable;
Sensitive Personal Data	which in the GDPR is referred to as "special categories of personal data" has the meaning set out in the Data Protection Legislation;
Standard Contractual Clauses	means (i) the Standard Contractual Clauses approved by the Commission for transfers from data controllers in the EEA to data controllers outside the EEA; and/or (ii) the Standard Contractual Clauses approved by the Commission for transfers from data controllers in the EEA to data processors outside the EEA each as updated and/or amended from time to time;
Third Party Request	means a written request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by law or regulation.

2. Interpretation

(a) Clause and Schedule headings are inserted for convenience only and shall not affect the interpretation of this Agreement.

(b) References to Clauses and Schedules are to the Clauses and Schedules of this Agreement.

(c) A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time.

(d) A reference to a statute or statutory provision shall include all subordinate legislation made under that statute or statutory provision.

(e) Any words following the terms including, include, in particular or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

(f) Words in the singular shall include the plural and in the plural include the singular.

Schedule 2: Data Protection Particulars

Subject matter of the processing:

The subject matter is the Processing of Personal Data for the purpose of executing planning simulations for therapeutic ultrasound treatments in the brain.

Duration of the processing:

Data processing will continue for the duration of use of the k-Plan software.

Nature and purpose of the processing:

k-Plan is used to execute cloud-based planning simulations for therapeutic ultrasound treatments in the brain on behalf of the End User. Medical images of the head and brain are added to the local installation of k-Plan by the End User, and then transferred to remote servers, which automatically process the data and execute planning simulations.

The medical image data along with the therapy settings are saved into a Planning File in a proprietary file format. The Planning File is pseudonymised and does not contain any identifiable information except for the raw medical image data. The code which links the Planning File with information about the data subject is only stored locally within the End User's installation of k-Plan.

To evaluate the plan, the End User selects to transmit the Planning File to the k-Plan remote servers and the plan is then scheduled for execution. When the execution is complete, the results are saved into a Results File in a proprietary file format. This contains information about the predicted ultrasound and thermal exposures for the treatment.

The End User can query the status of a plan via their local k-Plan installation. When the simulation is complete, the End User can select to download the Results File. The results are then displayed within the local installation of k-Plan for review by the End User.

The remote servers used by k-Plan are not a data storage system. The Planning File and Results File are only stored temporarily while being processed. After processing is complete, the files are securely deleted.

k-Plan uses servers that are located within the United Kingdom and the European Union. Depending on availability, the plans are executed on different high-performance computing servers, for example, servers available through the Amazon Elastic Compute Cloud, or the IT4Innovations National Supercomputing Center. Access to the End User data is protected and restricted to authorised administrators only.

Type of personal data:

The personal data being processed consists of medical images of the head and brain.

Categories of data subject:

The categories of data subjects are persons who have their medical image data entered into k-Plan by the End User.

Obligations and rights of the Data Controller:

These are as set out in the Agreement and this Schedule.

Sensitive Personal Data to be encrypted (if any):

Medical image data stored within the Planning File.

Methods and standards of encryption used:

Data transfers between the local k-Plan installation and the remote dispatch servers are performed using HTTPS communication protocols encrypted using Transport Layer Security (TLS). Data at rest on the remote dispatch servers is stored on an encrypted drive using AES-256 encryption. Data transfers between the remote dispatch servers and the compute servers use encrypted SSH connections.