EXHIBIT A

DATA PROCESSING ADDENDUM

The purpose of this Data Processing Addendum ("**DPA**") is to set out each party's obligations relating to the personal data processed by the parties pursuant to the agreement for the provision of certain services ("**Agreement**") entered into between them and to which this DPA is attached and incorporated.

1. DEFINITIONS

Defined terms in this DPA shall have the same meaning as set out in the Agreement unless otherwise defined below.

Appropriate Safeguards means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time.

Applicable Law means as applicable and binding on Customer, the Supplier and/or the Services:

(a) any law, statute, regulation, by-law or subordinate legislation in force from time to time to which a party is subject;

(b) any court order, judgment or decree; or

(c) any direction, policy, rule or order that is made or given by any regulatory body having jurisdiction over a party.

Controller means the entity which determines the purposes and means of the Processing of Personal Data.

Customer means the party named or identified as such in the Agreement being the recipient of the Services.

Data Subject means the identified or identifiable person to whom Personal Data relates.

Data Subject Request means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws.

Data Protection Laws means as applicable and binding on Supplier and the Customer in relation to the Services:

(a) in the United Kingdom the Data Protection Act 2018; and

(b) in member states of the European Union the GDPR and all relevant member state laws or regulations transposing or giving effect to or corresponding with GDPR.

Data Protection Losses means all losses and liabilities, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, expenses, losses and damages; and

(b) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; and

(c) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and

(d) the reasonable costs of compliance with investigations by a Supervisory Authority;

(e) costs of investigation including forensic investigation;

(f) cost of breach notification including notifications to the Data Subjects; and

(g) cost of complaints handling including providing Data Subjects with credit reference checks, setting up contact centres (e.g. call centres), producing end customer communication materials, provision of insurance to end customers (e.g. identity theft), and reimbursement of costs incurred by end customers (e.g. changing locks).

GDPR means the General Data Protection Regulation (EU) 2016/679.

Personal Data means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws.

Personal Data Breach means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data.

Processor means the entity which Processes Personal Data on behalf of the Controller.

processing means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (and related terms such as **process** have corresponding meanings).

Processing Instructions has the meaning given to that term in clause 3.2.

Protected Data means Personal Data in Captured Data provided to the Supplier by the Customer, or otherwise received by the Supplier in connection with the Services, pursuant to the Agreement.

SCCs means the European Commission approved Standard Contractual Clauses for the transfer of Personal Data from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws of the foregoing territories.

Services means the services provided to Customer by the Supplier pursuant to the Agreement.

Sub-Processor means another Processor engaged by the Supplier for carrying out processing activities in respect of the Protected Data on behalf of the Supplier.

Supervisory Authority means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.

Supplier means the party named or identified as such in the Agreement being the provider of the Services.

2. ROLES AND OBLIGATIONS

2.1 The parties agree that, for the Protected Data, Customer shall be the Controller and the Supplier shall be the Processor.

2.2 The Supplier shall process the Protected Data in compliance with:

(a) the obligations of Processors under Data Protection Laws and so as always not to place Customer in breach of Customer's obligations as a Controller of that Protected Data (subject to Customer complying with Data Protection Laws); and

(b) the terms of this DPA.

2.3 Customer shall ensure all data it provides to the Supplier for use in connection with the Services shall be collected and transferred to the Supplier in accordance with Data Protection Laws. For the avoidance of doubt, it shall be Customer's responsibility to (i) ensure the terms of use it supplies to the Data Subjects of the Protected Data comply with Data Protection Laws including in particular any fair processing information requirements relating to the processing of the Protected Data by the Supplier and (ii) to ensure it has a legal basis for the processing of the Protected Data by the Supplier.

2.4 Customer shall have sole responsibility for the accuracy, quality, and legality of Protected Data and the means by which Customer acquired Personal Data.

2.5 Customer shall obtain valid consents from Data Subject for the collection and transfer of Protected Data to the Supplier for processing as contemplated under the Agreement.

3. INSTRUCTIONS

3.1 Customer's instructions for the Processing of Protected Data shall comply with Data Protection Law.

3.2 Insofar as the Supplier processes Protected Data, the Supplier:

(a) shall (and shall ensure each person acting under its authority shall) process the Protected Data only on and in accordance with Customer's documented instructions from time to time and in accordance with Exhibit 1 (Data Processing Particulars), as updated from time to time by written agreement of the parties or as otherwise detailed in the Agreement ("**Processing Instructions**");

(b) shall inform Customer if the Supplier is aware of a Processing Instruction that, in its opinion, infringes Data Protection Laws.

4. TECHNICAL AND ORGANISATIONAL MEASURES

4.1 The Supplier shall implement and maintain, at its cost and expense:

(a) the technical and organisational measures prescribed by Data Protection Laws; and

(b) taking into account the nature of the processing, the technical and organisational measures necessary to assist Customer insofar as is reasonably possible in the fulfilment of Customer's obligations to respond to Data Subject Requests relating to Protected Data.

5. SUB PROCESSORS AND STAFF

5.1 The Supplier has appointed those Sub-Processor(s) listed in Exhibit 1 to this DPA under a written contract containing materially equivalent obligations to those in this DPA. Supplier shall provide Customer with a copy of the agreements with Sub-Processors if requested to do so by Customer. Supplier may redact commercial terms from such agreements before disclosing them to Customer.

5.2 The Supplier shall ensure that all of its personnel and contractors processing Protected Data are subject to a binding written contractual obligation with the Supplier or under professional obligation to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Supplier shall, where practicable and not prohibited by Applicable Law, notify Customer of any such requirement before such disclosure).

5.3 Supplier may not change or add new Sub-Processors without first notifying the Customer and giving the Customer ten days (from date of receipt of the notice) to object to the change or addition in Sub-Processor on reasonable and objectively justifiable grounds.

6. DATA SUBJECT REQUEST ASSISTANCE

6.1 Supplier shall promptly refer all Data Subject Requests it receives to Customer (wherever practicable within two working days of receipt of the request).

6.2 The Supplier shall provide such assistance to Customer as Customer reasonably requires (taking into account the nature of processing and the information available to the Supplier) to ensure compliance with each party's obligations under Data Protection Laws with respect to:

(a) Data Subject Requests;

(b) security of processing;

(c) data protection impact assessments (as such term is defined in Data Protection Laws);

(d) prior consultation with a Supervisory Authority regarding high risk processing; and

(e) notifications to the Supervisory Authority and/or communications to Data Subjects by Customer in response to any Personal Data Breach and for the avoidance of doubt the Supplier must promptly notify Customer in writing of any communications received by it from Data Subjects or Supervisory Authorities relating to the Protected Data without responding to either of the same unless it has been expressly authorised to do so by Customer.

7. OVERSEAS TRANSFERS

7.1 To the extent required under Data Protection Laws, Supplier shall ensure that any transfers (and any onward transfers) of Protected Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland

and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws of the foregoing territories, are effected by way of Appropriate Safeguards and in accordance with such Data Protection Laws.

8. RECORDS AND AUDITS

8.1 The Supplier shall maintain written records of all categories of processing activities carried out on behalf of Customer.

8.2 The Supplier shall make available to Customer such information as is reasonably necessary to demonstrate its compliance with the obligations of Processors under Data Protection Laws, and shall allow for and contribute to audits, including inspections, by Customer (or another auditor mandated by Customer) for this purpose, subject to Customer:

(a) giving the Supplier at least 30 days' advance notice of such information request, audit and/or inspection being required; and

(b) Customer and Supplier mutually agreeing the scope, timing, and duration of the audit; and

(c) ensuring that all information obtained or generated by Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law). Customer shall provide a copy of such information and audit reports to the Supplier following an inspection or audit pursuant to this clause 8.

9. BREACH NOTIFICATION

9.1 In respect of any Personal Data Breach involving Protected Data, the Supplier shall without undue delay and within 24 hours of becoming aware of the Personal Data Breach:

(a) notify Customer of the Personal Data Breach; and

(b) so far as possible without prejudicing the continued security of the Protected Data or any investigation into the Personal Data Breach, provide Customer with details of the Personal Data Breach.

10. DELETION OR RETURN OF DATA

10.1 The Supplier shall return all the Protected Data to Customer the earlier of:

(a) the end of the provision of the relevant Services related to processing of that Protected Data; or

(b) once processing by the Supplier of any Protected Data is no longer required for the purpose of Supplier's performance of its obligations under the Agreement.

11. LIABILITY

11.1 If a party receives a compensation claim from a person (including but not limited to a Data Subject) relating to processing of Protected Data processed by the Supplier under this Agreement, it shall promptly provide the other party with notice and full details of such claim. The Supplier shall make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of Customer.

11.2 This clause 11 does not affect the liability of the Supplier to any Data Subject or Supervisory Authority pursuant to a claim made directly against the Supplier by either of them.

11.3 As between the Supplier and the Customer liability for all Data Protection Losses arising out of any breach of this Data Processing Addendum including for any loss or damage arising out of a Personal Data Breach, shall be subject to the same caps and exclusions on liability as set out in the Agreement.

12. CHANGE IN LAW

Notwithstanding anything to the contrary in this DPA, in the event: (i) of a change in any law or regulation or (ii) a regulator issues a binding instruction, order or requirement which changes the basis on which the Protected Data can be processed, transferred or stored pursuant to this DPA, the parties agree to negotiate in good faith to agree an amendment to this DPA and that Agreement (to the extent necessary) to address change in law or regulation or to comply a binding instruction, order or requirement as applicable.

13. STANDARD CONTRACTUAL CLAUSES ADDITIONAL APPICATION

The parties agree to execute the European Union Standard Contractual Clauses (SCCs) attached in Exhibit 2, to apply only if Article 44 of GDPR applies to transfers of Protected Data from the European Economic Area to the United Kingdom in the event that: (a) the United Kingdom has left the European Union; and (b) and the transfer is not permitted under Article 45 of GDPR (transfers on the basis of an adequacy decision) or an European Union decision or agreement of equivalent effect.

EXHIBIT 1
DATA PROCESSING PARTICULARS

1. **Subject-matter of processing:**

   Data of customers of Customer in pseudonymised format and images for analysis of hearing health

2. **Duration of the processing:**

   Subject to Clause 10 of this DPA, Supplier will Process Personal Data for so long as necessary to perform the Services, unless otherwise agreed upon in writing.

3. **Nature and purpose of the processing:**

   To use the Protected Data for the purpose of providing the Services and as otherwise detailed in the Agreement, and as further instructed by Customer in its use of the Services.

4. **Type of Personal Data:**

   - Date of birth;
   - Sex;
   - Electronic media of Tympanic Membrane (ear drum) and ear canal;

   Special Category Data:

- ethnic origin;
- current medication;
- health status;
- medical history;

5. **Categories of Data Subjects:**

   - Individuals undergoing hearing health clinic

6. **Processing Instructions**

   To use the Protected Data for the purpose of providing the Services and as otherwise detailed in the Agreement.

7. **Sub-Processors**

Name	**Location**	**Processing Activity**
Google Inc (Google Cloud)	London, United Kingdom	Cloud hosting provider (with no logical access to data)

EXHIBIT 2

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The following information will be required in writing. Please contact us back for more information:

Name of the data exporting organisation
Address
Telephone
Fax
Email
Any other information

Name of the data importing organisation:
Address
Telephone
Fax
Email
Any other information

each "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone);

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the sub processor'* means any processor engaged by the data importer or by any other sub processor of the data importer who agrees to receive from the data importer or from any other sub processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability

of the sub processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub processing, the processing activity is carried out in accordance with Clause 11 by a sub processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub processor agrees that the data

subject may issue a claim against the data sub processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub processor preventing the conduct of an audit of the data importer, or any sub processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely: England

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub processor which imposes the same obligations on the sub processor as are imposed on the data importer under the Clauses - This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision. Where the sub processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely England
4. The data exporter shall keep a list of sub processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter

that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

The following Signatures will be required in writing

On behalf of the data exporter:
Name (written out in full):
Position
Address
Other information necessary in order for the contract to be binding (if any)

On behalf of the data importer:
Name (written out in full)
Position
Address
Other information necessary in order for the contract to be binding (if any)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

See Exhibit 1 to the DPA

Categories of data

See Exhibit 1 to the DPA

Special categories of data (if appropriate)

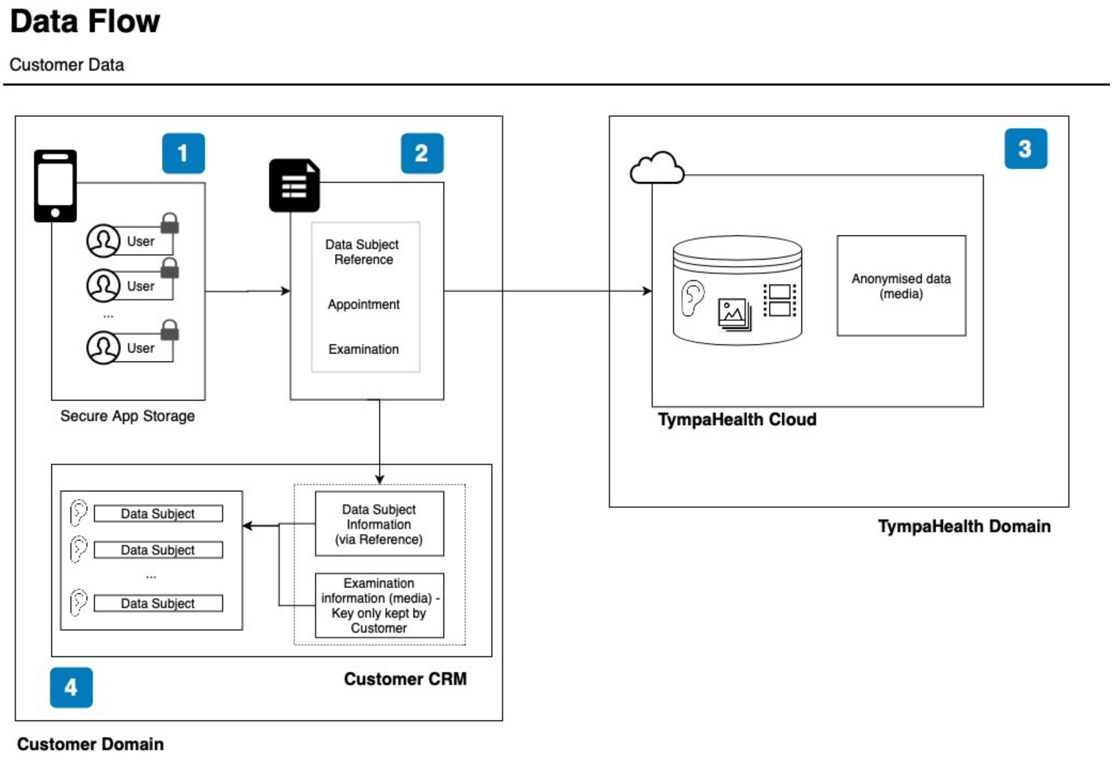
See Exhibit 1 to the DPA

Processing operations

See Exhibit 1 to the DPA

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties



1. All information captured in the app is stored in either database or files in the secure app storage area of the mobile operating system which is only accessible by the app. The files are separate for each logged in user in the app and loaded to phone memory upon user login (with pin or password).

2. The data stored contains data subject information, appointment details, examinations performed. All media captured during examination are also stored in the secure app documents storage area and are referenced to appointments and examinations by file name.

3. Data upload is performed using REST API using HTTPS protocol with latest TLS versions. When logging in, users are granted tokens which must be supplied when making calls to the APIs in request header. Without tokens the requests will fail. API uses Nginx web server with PHP running as fpm and stores information in Postgresql database. All internal traffic within cloud server infrastructure is internal and cannot be eavesdropped. Data uploaded to the Supplier domain is anonymised.

4. Data is retrieved using REST API using https protocol with latest TLS versions. Every request requires a valid token in the header. The token defines the scope of access to data. Tokens are granted by an Oath2 compatible authentication server. Supplying valid credentials creates and provides a JWS token which must be supplied in each API request. The tokens have limited lifespan and must be renewed when expired.