DATA PROCESSING ADDENDUM

Version 1.2 Last updated November 2026

1 General

This Data Processing Addendum (DPA) supplements the Master Subscription Terms (and any Order Form issued under the Master Subscription Terms), in respect of our Platform, (Terms) entered into between us and you. For the purposes of this DPA, we, us or our means HeartLab UK Ltd, a company incorporated in England and Wales with a company number of 16905949, and you or your means the customer listed in the Terms. We and you are together the Parties and each a Party. This DPA applies to our provision of the Platform (and any related services) (Services) to you under the Terms, from the date you agree to the Terms, and will continue in accordance with the terms of this DPA.

2 Definitions

2.1 Capitalised terms in this DPA have the meaning given in the Terms, the Annexures, and as set out below:

EU GDPR means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

EU SCCs means in respect of the **EU GDPR**, the standard contractual clauses annexed to the European Commission's implementing decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as may be amended, superseded or replaced from time to time.

Group Entities means any body corporate which is our holding company or subsidiary, and any other body corporate which is a subsidiary of our holding company, from time to time, including any of those entities listed in Annex 2.

Transferred Data means any Personal Data Processed by us or our Personnel on behalf of you in connection with the Terms.

Restricted Transfer means:

a where the **UK GDPR** applies, a transfer of personal data from the United Kingdom to any other country which is not subject to adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

b where the **EU GDPR** applies, a transfer of Personal Data from a country within the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission.

UK GDPR means the **EU GDPR** as incorporated into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.

UK Addendum means the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers approved by the Information Commissioner's Office under section 119A of the Data Protection Act 2018 on 21 March 2022 (version B.1.0), and as updated from time to time.

2.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processor", "Processing" and "Sub-Processor" shall have the same meaning as in the **UK GDPR**.

3 Roles of the Parties

The Parties acknowledge and agree that in connection with the Terms, where you provide us with **Transferred Data**, we are the Processor and you are the Controller.

4 Processing of Personal Data

4.1 Each Party agrees to comply with Applicable Data Protection Law in the Processing of **Transferred Data**.

4.2 You instruct us to process **Transferred Data** in accordance with this DPA (including in accordance with Annex 1). We agree to not process **Transferred Data** other than on your documented instructions (as set out in this DPA and the Terms).

5 Our Personnel

We agree to take reasonable steps to ensure the reliability of any of our Personnel who may have access to the **Transferred Data**, ensuring in each case that:

a access is strictly limited to those individuals who need to know / access the relevant **Transferred Data**, as strictly necessary for the purposes of the Terms; and

b the relevant Personnel are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6 Security

6.1 Taking 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, we agree to implement appropriate technical and organisational measures in relation to the **Transferred Data** to ensure a level of security appropriate to that risk in accordance with Applicable Data Protection Law.

6.2 In assessing the appropriate level of security, we agree to take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

7 Sub-Processing

7.1 You authorise the engagement of any of our **Group Entities** as our Sub-Processors where relevant to the Services.

7.2 Without limiting clause 7.1, you authorise our engagement of the Sub-Processors already engaged by us at the date of this DPA, which are set out at Annex 3.

7.3 Subject to clause 7.1, where we wish to engage a new Sub-Processor, we agree to provide written notice to you of the details of the engagement of the Sub-Processor at least 14 days' prior to engaging the new Sub-Processor (including details of the processing it will perform). You may object in writing to our appointment of a new Sub-Processor within 7 days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the Parties will discuss such concerns in good faith with a view to achieving resolution. If the Parties are not able to achieve resolution, we may, at our election:

a not appoint the proposed Sub-Processor;

b not disclose any **Transferred Data** we process on your behalf to the proposed Sub-Processor; or

c inform you that we may terminate the Terms (including this DPA) for convenience, in which case, clause 14.2 will apply.

7.4 You agree that the remedies described above in clause 7.3 are the only remedies available to you if you object to our engagement of any proposed Sub-Processor by us.

7.5 Where we engage a Sub-Processor to process **Transferred Data**, we agree to enter into a written agreement with the Sub-Processor (which may be a data sharing agreement, in the event that the Sub-Processor is one of our **Group Entities)** containing data protection obligations no less protective than those in this DPA with

respect to the **Transferred Data**, and to remain responsible to you for the performance of such Sub-Processor's data protection obligations under such terms.

7.6 Where the transfer of **Transferred Data** from us to a Sub-Processor is a **Restricted Transfer**, it will be subject to the **UK Addendum** (and documents or legislation referred to within it) and the **EU SCCs**, which shall be deemed to be incorporated into this DPA, and the **UK Addendum** and the **EU SCCs** are considered an appropriate safeguard.

8 Data Subject Rights

8.1 Taking into account the nature of the Processing, we agree to assist you by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of your obligations, as reasonably understood by you, to respond to requests to exercise Data Subject rights under the Applicable Data Protection Law.

8.2 We agree to:

a promptly notify you if we receive a request from a Data Subject under any Applicable Data Protection Law in respect of **Transferred Data**; and

b ensure that we do not respond to that request except on your documented instructions or as required by Applicable Data Protection Law to which we are subject, in which case we shall, to the extent permitted by Applicable Data Protection Law, inform you of that legal requirement before we (or our Sub-Processor) respond to the request.

9 Personal Data Breach

9.1 We agree to notify you without undue delay upon becoming aware of a Personal Data Breach affecting **Transferred Data**, and to provide you with sufficient information to allow you to meet any obligations to report or inform Data Subjects of the Personal Data Breach under Applicable Data Protection Law.

9.2 We agree to co-operate with you and take reasonable commercial steps as directed by you to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9.3 If you decide to notify a Supervisory Authority, Data Subjects or the public of a Personal Data Breach, you agree to provide us with advance copies of the proposed notices and, subject to Applicable Data Protection Law (including any mandated deadlines under the **UK GDPR**), allow us an opportunity to provide any clarifications or corrections to those notices.

10 Data Protection Impact Assessment and Prior Consultation

We agree to provide reasonable assistance to you with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which you reasonably consider to be required by article 35 or 36 of the **UK GDPR** or equivalent provisions of any other Data Protection Law (to the extent you do not otherwise have access to the relevant information and such information is in our control).

11 Deletion or return of Personal Data

Subject to any document retention requirements at law, we agree to promptly and in any event within 30 business days of the date of cessation of any Services involving the Processing of **Transferred Data** (**Cessation Date**), delete and procure the deletion of all copies of those **Transferred Data**.

12 Audit Rights

12.1 Subject to this clause 12, where required by law, we shall make available to you on request all information reasonably necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by you or an auditor mandated by you in relation to the Processing of Transferred Data by us.

12.2 Where clause 12.1 applies, any audit (or inspection):

a must be conducted during our regular business hours, with reasonable advance notice (which shall not be less than 30 business days);

b will be subject to our reasonable confidentiality procedures;

c must be limited in scope to matters specific to you and agreed in advance with us;

d must not require us to disclose to you any information that could cause us to breach any of our obligations under Applicable Data Protection Law;

e to the extent we need to expend time to assist you with the audit (or inspection), this will be funded by you, in accordance with pre-agreed rates; and

f may only be requested by you a maximum of one time per year, except where required by a competent Supervisory Authority or where there has been a Personal Data Breach in relation to Transferred Data, caused by us.

12.3 Your information and audit rights only arise under clause 12.1 to the extent that the Terms do not otherwise give you information and audit rights that meet the relevant requirements of Applicable Data Protection Law.

13 Liability

Despite anything to the contrary in the Terms or this DPA, to the maximum extent permitted by law, the Liability of each Party and its affiliates under this DPA is subject to the exclusions and limitations of Liability set out in the Terms.

14 Termination

14.1 Each Party agrees that a failure or inability to comply with the terms of this DPA and/or the Applicable Data Protection Law constitutes a material breach of the Terms. In such event, you may, without penalty:

a require us to suspend the processing of **Transferred Data** until such compliance is restored; or

b terminate the Terms effective immediately on written notice to us.

14.2 In the case of such suspension or termination by you, we shall provide a prompt pro-rata refund of all sums paid in advance under the Terms which relate to the period of suspension or the period after the date of termination (as applicable).

14.3 Notwithstanding the expiry or termination of this DPA, this DPA will remain in effect until, and will terminate automatically upon, deletion by us of all **Transferred Data** covered by this DPA, in accordance with this DPA.

ANNEX 1 DESCRIPTION OF TRANSFER

Personal Data Transferred	• Identity Data including first name, last name, title, and job title. • Contact Data including billing addresses, delivery addresses, email addresses and telephone numbers. • Employee details including Identity Data and Contact Data of past, present and future employees. • Financial Data including bank account and payment card details. • Background Verification Data including passport numbers, driver licence numbers, photographic identification, anti-money laundering laws and related ongoing monitoring commitments.
Special Categories of Personal Data and criminal convictions and offences	The transferred data includes special category data relating to: • racial or ethnic origin • genetic data • physical or mental health
Relevant Data Subjects	• business contact representatives; • your staff members; • your customers; • anyone about whom personal data is input into the Services; and • authorised users of the Services.
Frequency of the transfer	Continuous
Nature of the transfer	As specified in the Terms and this DPA, including without limitation: • use, collection, organisation, storage (hosting), retrieval and other processing by us of **Transferred Data** to provide, maintain and improve the Services; • transmission, disclosure and dissemination of Transferred Data to provide the Services in accordance with the Terms; and • as compelled by law.
Purpose of processing	The purpose of the transfer and processing are as specified in the Terms, any applicable quote, Service Order and/or Statement of Work and this DPA.
Duration of the Processing	The term of the Terms, and for a period of 30 days after termination or expiry of the Terms, unless otherwise required by law.

ANNEX 2 GROUP ENTITIES

GROUP ENTITY	LOCATION
HeartLab, Inc., a company incorporated in the state of Delaware	USA
HeartLab Australia Pty Ltd, a company incorporated in the state of New South Wales, Australia (ABN 20 675 520 448)	Australia
HeartLab UK Ltd, a company incorporated in England and Wales (company number 16905949)	United Kingdom
HeartLab Limited, a company incorporated in New Zealand (NZBN 9429046990761)	New Zealand

ANNEX 3 LIST OF SUB-PROCESSORS

SUB-PROCESSOR	DESCRIPTION OF SERVICE	LOCATION	USED FOR	WEBSITE & CONTACT DETAILS
Amazon Web Services (AWS) eu-west-2	Cloud infrastructure; database hosting, S3 storage, compute (Lambda, Fargate, ECS) for processing and storing all patient/clinical data	United Kingdom (London)	Primary cloud hosting environment for all patient and clinical data; DICOM storage and processing; database hosting; application compute; backup and disaster recovery.	https://aws.amazon.com Privacy & GDPR: https://aws.amazon.com/compliance/gdpr-center/ DPA: https://aws.amazon.com/agreement/
Plain (Not Just Tickets Ltd)	Cloud-based customer support platform. Support requests submitted by HeartLab customers may contain personal data relating to users or patients.	United Kingdom (primary hosting); United States of America (supporting services, including email delivery)	Customer support ticket management and customer communications.	https://www.plain.com Privacy Policy: https://www.plain.com/legal/privacy-policy DPA: https://www.plain.com/legal/dpa
Google Workspace (Google LLC)	Cloud-based productivity and collaboration suite.	United States of America (USA)	Customer support ticketing via the help@heartlab.com email address	https://workspace.google.com Privacy Policy: https://policies.google.com/privacy DPA: https://workspace.google.com/terms/dpa_terms.html