Kardiaport Data Processing Policy

Definitions

In this Agreement:

Applicable Law	means the following to the extent forming part of the law of the United Kingdom (or a part of the United Kingdom) as applicable and binding on either party or the Services: (a) any law, statute, regulation, byelaw or subordinate legislation in force from time to time; (b) the common law and laws of equity as applicable to the parties from time to time; (c) any binding court order, judgment or decree; or (d) any applicable direction, policy, rule or order made or given by any regulatory body having jurisdiction over a party or any of that party's assets, resources or business
Attached Standard Contractual Clauses	means the provisions set out in *Annex 1* to Schedule 4;
Controller	has the meaning given to that term in Data Protection Laws;
Data Protection Laws	means as applicable and binding on either party or the Services: (a) the GDPR; (b) the Data Protection Act 2018; and (c) any laws that supplement, replace, extend, re-enact, consolidate or amend any of the foregoing
Data Protection Losses	means all liabilities, including all: (a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and

(b) to the extent permitted by Applicable Law:

(i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Data Protection Supervisory Authority;

(ii) compensation which is ordered by a court or Data Protection Supervisory Authority to be paid to a Data Subject; and

(iii) the reasonable costs of compliance with investigations by a Data Protection Supervisory Authority;

Data Protection 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;

Data Subject has the meaning given to that term in Data Protection Laws;

Data Subject Request means a request made by a Data Subject to exercise any rights of Data Subjects under Chapter III of the GDPR in relation to any Protected Data;

GDPR means the General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time);

International Recipient means the organisations, bodies, persons and other recipients to which Transfers of Protected Data are prohibited under clause 6.1 without the Processor's prior written authorisation;

Lawful Safeguards means such legally enforceable mechanism(s) for Transfers of Personal Data as may be permitted under Data Protection Laws from time to time;

Onward Transfer means a Transfer from one International Recipient to another International Recipient;

Personal Data	has the meaning given to that term in 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;
Processing	has the meaning given to that term in Data Protection Laws (and related terms such as **process**, **processes** and **processed** have corresponding meanings);
Processing End Date	means the earlier of: (a) the end of the provision of the relevant Services related to processing of the Protected Data; or (b) once processing by the Processor of any Protected Data is no longer required for the purpose of the Processor's performance of its relevant obligations under this Agreement;
Processing Instructions	has the meaning given to that term in clause 2.1.1;
Processor	has the meaning given to that term in Data Protection Laws;
Protected Data	means Protected Data means Personal Data received from or on behalf of the Controller in connection with the performance of the Processor's obligations under this Agreement.
Sub-Processor	means Processor engaged by the Processor or by any other Sub-Processor for carrying out processing activities in respect of the Protected Data on behalf of the Controller; and
Transfer	bears the same meaning as the word 'transfer' in Article 44 of the GDPR. Related expressions such as **Transfers** and **Transferring** shall be construed accordingly

Specific interpretive provision(s)

In this Agreement:

(a) references to any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting or consolidating such

Applicable Law (including any new Data Protection Laws from time to time) and the equivalent terms defined in such Applicable Laws, once in force and applicable;

(b) a reference to a law includes all subordinate legislation made under that law; and

(c) a reference to 'writing' or 'written' includes any method of reproducing words in a legible and non-transitory form;

Data processing provisions

1 Processor and Controller

1.1 The Controller is Kardiaport, the entity that determines the purposes and means of processing the Protected Data (e.g. the research sponsor or client). The Controller is responsible for ensuring compliance with the UK GDPR, including the principles of data protection and accountability. The Processor shall assist the Controller in fulfilling these obligations as outlined in this Agreement.

1.2 Kardiaport shall act as the Processor, processing the Protected Data on behalf of the Controller in accordance with this Agreement and the Controller's documented instructions.

1.3 To clarify, Kardiaport acts as both the Controller and the Processor under this Agreement. As the Controller, Kardiaport determines the purposes and means of processing the Protected Data. As the Processor, Kardiaport carries out the processing activities in accordance with its own documented instructions and the terms of this Agreement.

1.4 The Participant (individuals providing their data) are the Data Subjects under Data Protection Laws.

1.5 The Controller shall ensure that fair processing notices are provided to Data Subjects and that all necessary consents are obtained and maintained, as required by Data Protection Laws.

1.6 The Processor shall process Protected Data in compliance with:

1.1.1 the obligations of Processors under Data Protection Laws in respect of the performance of its obligations under this Agreement; and

1.1.2 the terms of this Agreement.

1.7 The Processor shall comply with:

1.7.1 all Data Protection Laws in connection with the processing of Protected Data, the Services and the exercise and performance of its respective rights and obligations under this Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

1.1.3 the terms of this Agreement.

1.8 The Processor warrants, represents and undertakes, that at all times:

1.8.1 the processing of all Protected Data (if processed in accordance with this Agreement) shall comply in all respects with Data Protection Laws, including in terms of its collection, use and storage;

1.8.2 fair processing and all other appropriate notices have been provided to the Data Subjects of the Protected Data (and all necessary consents from such Data Subjects obtained and at all times maintained) to the extent required by Data Protection Laws in connection with all processing activities in respect of the Protected Data which may be undertaken by the Processor and its Sub-Processors in accordance with this Agreement;

1.8.3 the Protected Data is accurate and up to date;

1.8.4 except to the extent resulting from Transfers to International Recipients made by the Processor or any Sub-Processor, the Protected Data is not subject to the laws of any jurisdiction outside of the United Kingdom;

1.8.5 it shall establish and maintain adequate security measures to safeguard the Protected Data in its possession or control (including from unauthorised or unlawful destruction, corruption, processing or disclosure);

1.8.6 it shall maintain complete and accurate backups of all Protected Data provided to the Processor (or anyone acting on its behalf) so as to be able to immediately recover and reconstitute such Protected Data in the event of loss, damage or corruption of such Protected Data by the Processor or any other person;

1.8.7 all instructions given by it to the Processor in respect of Personal Data shall at all times be in accordance with Data Protection Laws; and

1.8.8 it is satisfied that:

(a) the Processor's processing operations are suitable for the purposes for which the Processor proposes to use the Services and engage the Processor to process the Protected Data;

(b) the technical and organisational measures set out in Schedule 3 shall (if the Processor complies with its obligations under such Schedule) ensure a level of security appropriate to the risk in regards to the Protected Data as required by Data Protection Law; and

(c) the Processor has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

1.9 The Processor shall not unreasonably withhold, delay or condition its agreement to any Change requested by the Processor in order to ensure the Services and the Processor (and each Sub-Processor) can comply with Data Protection Laws.

1.10 The Processor shall only process Protected Data in accordance with the Controller's documented instructions. If the Processor determines the purposes and means of processing outside of these instructions, it shall be considered a Controller for that processing and assume the associated responsibilities.

2 Instructions and details of processing

2.1 Insofar as the Processor processes Protected Data on behalf of the Processor, the Processor:

2.1.1 unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Processor's documented instructions as set out in this Agreement (including with regard to a Transfer of Protected Data to any International Recipient), as updated from time to time in accordance with the Change Control Procedure (Processing Instructions);

2.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Processor of any such requirement before processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and

2.1.3 shall promptly inform the Processor if the Processor becomes aware of a Processing Instruction that, in the Processor's opinion, infringes Data Protection Laws, provided that:

(a) this shall be without prejudice to clauses 1.7 and 1.8; and

(b) to the maximum extent permitted by Applicable Law, the Processor shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Processing Instructions following the Processor's receipt of that information.

2.2 The processing of Protected Data to be carried out by the Processor under this Agreement shall comprise the processing set out in Schedule 1, as may be updated from time to time in accordance with the Change Control Procedure.

3 Technical and organisational measures

3.1 The Processor shall implement and maintain, at its cost and expense, technical and organisational measures:

3.1.1 in relation to the processing of Protected Data by the Processor, as set out in Schedule 3; and

3.1.2 taking into account the nature of the processing, to assist the Processor insofar as is possible in the fulfilment of the Processor's obligations to respond to Data Subject Requests relating to Protected Data. The parties have agreed that (taking into account the nature of the processing) the Processor's compliance with clause 5.1 shall constitute the Processor's sole obligations under this clause 3.1.2.

3.2 Any additional technical and organisational measures shall be at the Processor's cost and expense.

4 Using staff and other Processors

4.1 Subject to clause 4.2, The Processor shall not engage (nor permit any other Sub-Processor to engage) any Sub-Processor for carrying out any processing activities in respect of the Protected Data without the Controller's prior written authorisation of that specific Sub-Processor.

4.2 The Processor authorises the appointment of the Sub-Processors listed below:

Sub-Processor	Processing this Sub-Processor is authorised to undertake	Country/ies where processing by this Sub-Processor may take place
Microsoft Azure, a company incorporated in the United States under Microsoft Corporation, Redmond, WA 98052-6399, USA	Secure storage and hosting of Protected Data	United Kingdom (primary), European Economic Area (EEA), United States

4.3 The Processor shall reply to any communication from the Processor requesting any further prior specific authorisation of a Sub-Processor pursuant to clause 4.1 promptly and in any event within 10 Business Days of request from time to time. The Processor shall not unreasonably withhold, delay or condition any such authorisation.

4.4 In the event the Processor fails to comply with any of its obligations in clause 4.3 or withholds any requested authorisation further to clause 4.3, the Processor may terminate this Agreement with an immediate notice..

4.5 The Processor shall:

4.5.1 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, ensure each Sub-Processor is appointed under a written contract containing materially the same obligations as under clauses 1 to 11 (inclusive) (including those obligations relating to sufficient guarantees to implement appropriate technical and organisational measures) that is enforceable by the Processor;

4.5.2 ensure each such Sub-Processor complies with all such obligations; and

4.5.3 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

4.6 The Processor shall ensure that all persons authorised by it (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Processor shall, where practicable and not prohibited by Applicable Law, notify the Processor of any such requirement before such disclosure).

5 Assistance with the Processor's compliance and Data Subject rights

5.1 The Processor shall refer all Data Subject Requests it receives to the Controller within ten Business Days of receipt of the request. The Controller remains responsible for responding to such requests in compliance with Data Protection Laws, within ten Business Days of receipt of the request, provided that if the number of Data Subject Requests exceeds ten per calendar month, the Processor shall pay the Processor for all work, time, costs and expenses incurred by the Processor or any Sub-Processor(s) in connection with all further Data Subject Requests in such month calculated on a time and materials basis at the Processor's rates set out in Schedule 2.

5.2 The Processor shall provide such assistance as the Processor reasonably requires (taking into account the nature of processing and the information available to the Processor) to the Processor in ensuring compliance with the Processor's obligations under Data Protection Laws with respect to:

5.2.1 security of processing;

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

5.2.3 prior consultation with a Data Protection Supervisory Authority regarding high risk processing; and

5.2.4 notifications to the Data Protection Supervisory Authority and/or communications to Data Subjects by the Processor in response to any Personal Data Breach,

provided the Processor shall pay the Processor for all work, time, costs and expenses incurred by the Processor or any Sub-Processor(s) in connection with providing the assistance in this clause 5.2 and clause 5.3, such Charges to be calculated on a time and materials basis at the Processor's rates set out in Schedule 2.

5.3 The assistance referred to in clause 5.2 shall include the assistance set out in Schedule 6.

5.4 The Controller has designated Ms. Isabel Al-Dhahir to handle all Data Subject Requests directly. The Processor shall provide all necessary assistance to Isabel to ensure timely and accurate responses to such requests.

5.5 The Processor shall refer all Data Subject Requests to the Controller within ten Business Days of receipt of the request. The Controller shall respond to such requests within the standard response window of 10 Business Days, unless otherwise required by Applicable Law.

6 International Transfers

6.1 Subject to clause 6.2, the Processor shall not Transfer (nor permit any Onward Transfer of) any Protected Data:

6.1.1 to any country or territory outside the United Kingdom; and/or

6.1.2 to an organisation and/or its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries,

without the Processor's prior written authorisation except where required by Applicable Law (in which case the provisions of clause 2.1 shall apply).

6.2 The Processor hereby authorises the Processor (or any Sub-Processor) to Transfer Protected Data for the purposes referred to in Schedule 4 in accordance with that Schedule, provided all Transfers of Protected Data by the Processor of Protected Data to an International Recipient (including any Onward Transfer) shall:

6.2.1 be effected by way of the Lawful Safeguards referred to in clause 6.3 and in accordance with this Agreement; and

6.2.2 be made pursuant to a written contract, including equivalent obligations on each Sub-Processor in respect of Transfers to International Recipients as apply to the Processor under any of this clause 6.

The provisions of this Agreement shall constitute the Processor's instructions with respect to Transfers of Protected Data to International Recipients for the purposes of this Agreement.

6.3 The Lawful Safeguards employed by the Processor in connection with this Agreement shall be:

6.3.1 as set out in Schedule 4; or

6.3.2 an alternative Lawful Safeguard agreed under the Change Control Procedure (consent of either party not to be unreasonably, withheld, conditioned or delayed).

6.4 The Processor and each Sub-Processor is not obliged to make any unlawful Transfer of Protected Data and shall not be liable to the extent that it (or any Sub-Processor) is delayed in or fails to perform any obligation under this Agreement due to:

6.4.1 there being no available valid Lawful Safeguard agreed under clause 6.3 from time to time for any of the Transfers authorised pursuant to clause 6.2 ; or

6.4.2 the Processor or any Sub-Processor declining to permit any Transfer(s) on the basis it believes (acting reasonably) that the circumstances in clause 6.4.1 apply.

The Charges payable to the Processor shall not be discounted or set-off as a result of any delay or non-performance of any obligation in accordance with this clause 6.4.

7 Records, information and audit

7.1 The Processor shall maintain, in accordance with Data Protection Laws binding on the Processor, written records of all categories of processing activities carried out on behalf of the Processor.

7.2 The Processor shall, in accordance with Data Protection Laws, make available to the Processor such information as is reasonably necessary to demonstrate the Processor's compliance with its obligations under Article 28 of the GDPR, and allow for and contribute to audits, including inspections, by the Processor (or another auditor mandated by the Processor) for this purpose, subject to the Processor:

7.2.1 giving the Processor reasonable prior notice of such information request, audit and/or inspection being required by the Processor;

7.2.2 ensuring that all information obtained or generated by the Processor or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to a Data Protection Supervisory Authority or as otherwise required by Applicable Law);

7.2.3 hereby agreeing that the Processor shall be entitled to withhold *nformation where it is commercially sensitive or confidential to it or its other Processors*;

7.2.4 ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to the Processor's business, the Sub-Processors' businesses and the business of any Processors of the Processor or of any of the Sub-Processors; and

7.2.5 paying the Processor for all work, time, costs and expenses incurred by the Processor or any Sub-Processor(s) in connection with the provision of information and allowing for and contributing to inspections and audits, such Charges to be calculated on a time and materials basis at the Processor's rates set out in Schedule 2.

8 Breach notification

8.1 In respect of any Personal Data Breach, the Processor shall, without undue delay:

8.1.1 notify the Processor of the Personal Data Breach; and

8.1.2 provide the Processor with details of the Personal Data Breach.

9 Deletion or return of Protected Data and copies

9.1 Subject to clauses 9.2 and 9.3, the Processor shall retain and delete Protected Data in accordance with Schedule 5.

9.2 Subject to clause 9.3, the Processor shall (and shall ensure that each of the Sub-Processors shall) delete the Protected Data (and all copies) within a reasonable time after the Processing End Date except to the extent that storage of any such data is required by Applicable Law (and, if so, the Processor shall inform the Processor of any such requirement and shall (and shall ensure any relevant Sub-Processor shall) securely delete such data promptly once it is permitted to do so under Applicable Law).

9.3 The Processor shall promptly comply with any reasonable requests from time to time from the Processor for the secure return or transfer of Protected Data to the Processor within a reasonable time and provided:

9.3.1 such request is received within *six* Business Days of the relevant Processing End Date; and

9.3.2 the Processor shall pay the Processor for all work, time, costs and expenses incurred by the Processor or any Sub-Processor(s) in connection with such activity, such Charges to be calculated on a time and materials basis at the Processor's rates set out in Schedule 2.

10 Liability, indemnities and compensation claims

10.1 The Processor shall indemnify and keep indemnified the Processor in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, the Processor and any Sub-Processor arising from or in connection with any:

10.1.1 non-compliance by the Processor with the Data Protection Laws;

10.1.2 processing carried out by the Processor or any Sub-Processor pursuant to any Processing Instruction that infringes any Data Protection Law; or

10.1.3 breach by the Processor of any of its obligations under clauses 1 to 11 (inclusive),

except to the extent the Processor is liable under clause 10.2.

10.2 The Processor shall be liable for Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with this Agreement:

10.2.1 only to the extent caused by the processing of Protected Data under this Agreement and directly resulting from the Processor's breach of clauses 1 to 11 (inclusive); and

10.2.2 in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of this Agreement by the Processor (including in accordance with clause 2.1.3(b)).

10.3 If a party receives a compensation claim from a person relating to processing of Protected Data, it shall promptly provide the other party with notice and full details of such claim.

10.4 The parties agree that the Processor shall not be entitled to claim back from the Processor any part of any compensation paid by the Processor in respect of such damage to the extent that the Processor is liable to indemnify or otherwise compensate the Processor in accordance with clause 10.1.

10.5 This clause 10 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

10.5.1 to the extent not permitted by Applicable Law (including Data Protection Laws); and

10.5.2 that it does not affect the liability of either party to any Data Subject.

11 Survival of data protection provisions

11.1 Clauses 1 to 8 (inclusive) shall survive expiry or termination (for any reason) of this Agreement and continue until no Protected Data remains in the possession or control of the Processor or any Sub-Processor. The termination or expiry of such clauses shall be without prejudice to any accrued rights or remedies of either party under any such clauses at the time of such termination or expiry.

11.2 Clauses 9 to 11 (inclusive) shall survive expiry or termination (for any reason) of this Agreement and continue indefinitely.

12 Data protection contact

The Processor's *Data Protection Officer* may be contacted at contact@kardiaport.com (or via such other contact details as may be notified by the Processor to the Processor from time to time).

SCHEDULE 1
DATA PROCESSING DETAILS

1 Subject-matter of processing:

Health data collected from wearable devices and self-reported forms for research purposes.

2 Duration of the processing:

Until the conclusion of the research study or as required by law.

3 Nature and purpose of the processing:

Analysis of health data to gain insights into health and activity trends.

4 Type of Personal Data:

Health metrics, activity data, and Processor identifiers.

5 Categories of Data Subjects:

Research Processors aged 18 and above.

6 Special categories of Personal Data:

NA

7 Further Processing Instructions

NA

SCHEDULE 2
CHARGES

NA

SCHEDULE 3
TECHNICAL AND ORGANISATIONAL MEASURES

The Processor shall implement and maintain the following technical and organisational security measures to protect the Protected Data:

Encryption:

All Protected Data shall be encrypted both in transit (e.g., using TLS/SSL protocols) and at rest (e.g., AES-256 encryption) to prevent unauthorised access.

Encryption keys shall be securely managed and stored separately from the encrypted data.

Access Controls:

Role-based access controls (RBAC) shall be implemented to ensure that only authorised personnel have access to Protected Data.

Multi-factor authentication (MFA) shall be required for all personnel accessing systems that store or process Protected Data.

Data Anonymisation and Pseudonymisation:

Protected Data shall be anonymised or pseudonymised wherever possible to minimise risks in the event of unauthorised access.

Identifiers such as names shall be replaced with unique Processor codes (e.g. P1, P2).

Secure Storage:

Protected Data shall be stored on Microsoft Azure, which complies with GDPR and UK Data Protection Act 2018 requirements.

Data backups shall be encrypted and stored securely to ensure data recovery in the event of a system failure or breach.

Monitoring and Logging:

Continuous monitoring of systems shall be conducted to detect and respond to unauthorised access or suspicious activity.

Detailed logs of data access and processing activities shall be maintained and reviewed regularly.

Network Security:

Firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) shall be used to protect networks where Protected Data is processed or stored.

Regular vulnerability assessments and penetration testing shall be conducted to identify and address potential security risks.

SCHEDULE 4
INTERNATIONAL TRANSFERS

No international transfers of Protected Data are currently applicable under this Agreement. Should international transfers become necessary, they will be conducted in compliance with Data Protection Laws, including the implementation of Lawful Safeguards such as Standard Contractual Clauses or adequacy decisions.

SCHEDULE 5
DATA RETENTION

Retention Period:

Protected Data will be retained for the duration of the research study and for a period of 3 to 5 years following the conclusion of the study, or as required by contractual, legal, or regulatory obligations.

Requests for deletion of Protected Data will be fulfilled unless retention is required to comply with legal or regulatory obligations.

Anonymised Data:

Anonymised data, which cannot be traced back to individual Data Subjects, may be retained indefinitely for research and analysis purposes. Requests for deletion of Protected Data will not apply to anonymised data already integrated into research analysis.

Deletion of Data Upon Request:

Processors may request the deletion of their personal data at any time by contacting Kardiaport.

If the data has already been anonymised and integrated into research analysis, it may not be possible to delete it. Processors will be informed of any such limitations.

Secure Deletion:

Protected Data will be securely deleted using industry-standard methods, such as data wiping or shredding, to ensure it cannot be recovered.

Any physical copies of Protected Data will be destroyed using secure shredding processes.

Backup Data:

Backup copies of Protected Data will be retained only for disaster recovery purposes and will be securely deleted in accordance with the retention period outlined above.

Ongoing Review:

Data retention practices will be reviewed periodically to ensure compliance with legal and regulatory requirements.

Any changes to the retention policy will be communicated to Processors via the contact details they have provided.

SCHEDULE 6
ADDITIONAL ASSISTANCE

The Processor shall:

Data Subject Requests:

Assist Kardiaport in responding to Data Subject Requests, including requests for access, rectification, erasure, restriction, portability, or objection to the processing of Protected Data.

Provide all necessary information and tools to enable Kardiaport to fulfil such requests within the timeframes required by Data Protection Laws.

Data Protection Impact Assessments (DPIAs):

Provide reasonable assistance to Kardiaport in conducting Data Protection Impact Assessments (DPIAs) where required, including providing relevant information about processing activities and technical and organisational measures.

Assist in prior consultations with Data Protection Supervisory Authorities, if necessary, in relation to high-risk processing activities.

Personal Data Breaches:

Notify Kardiaport without undue delay of any Personal Data Breach and provide all relevant details, including:

- The nature of the breach;
- The categories and approximate number of Data Subjects affected;
- The categories and approximate number of data records affected;
- Likely consequences of the breach; and
- Measures taken or proposed to address the breach and mitigate its effects.

Assist Kardiaport in notifying the relevant Data Protection Supervisory Authority and/or affected Data Subjects, as required by law.

Audits and Inspections:

Allow Kardiaport or its authorised representatives to conduct audits and inspections of the Processor's data processing activities, subject to reasonable notice and during normal business hours.

Provide access to relevant records, systems, and personnel to demonstrate compliance with Data Protection Laws and the terms of this Agreement.

Technical and Organisational Measures:

Logs of data access and processing activities shall be retained for a minimum of 12 months to ensure compliance and facilitate audits.

Anonymisation will be used wherever possible to minimise risks, especially for research purposes.

Training and Awareness:

Ensure that all personnel authorised to process Protected Data are trained on data protection principles and are aware of their obligations under this Agreement and Data Protection Laws.

International Transfers:

Assist Kardiaport in ensuring that any international transfers of Protected Data comply with applicable legal requirements, including the implementation of Lawful Safeguards such as Standard Contractual Clauses or adequacy decisions.

Policy Updates and Compliance:

The Processor shall notify the Controller of any changes in Data Protection Laws that may affect the processing of Protected Data. The Processor shall deliver updated policies and documents to the Controller for review within 10 Business Days of identifying the need for revision.

Data Retention and Deletion:

Assist Kardiaport in securely deleting or returning Protected Data upon request or at the end of the retention period, as outlined in this Agreement.

Costs and Charges:

The Processor shall assist the Controller in responding to Data Subject Requests, including requests for access, rectification, erasure, restriction, portability, or objection to the processing of Protected Data. The Controller remains responsible for fulfilling such requests.

Any additional assistance beyond the scope of this Agreement shall require prior written approval from the Controller and may be subject to reasonable charges, calculated on a time and materials basis at the Processor’s standard rates.