DATA SHARING AGREEMENT

THIS AGREEMENT is made the on ___ _____ 2024

BETWEEN:

(1) LONGEVITY CARD LTD, private limited liability company incorporated and existing under the laws of England and Wales, registered with the Companies House under registration number 12506506, having its registered office at 85 Great Portland Street, London, England, W1W 7LT (hereinafter referred to as “Supplier” or “Party 1”), on behalf of itself and its affiliates, and

(2) [name of Supplier], private limited liability company incorporated and existing under the laws of England and Wales, registered under the registration number [company No.], having its registered office at [address] (hereinafter referred as “Customer” or “Party 2”), each a "**Party**" and together the "**Parties**".

RECITALS:

(A) For the purpose of providing the Services under the White Label Soluton Agreement dated __ _____ 2024 both Parties may receive personal Data.

(B) The Parties have entered into this Agreement (as defined below) to provide for the sharing of Personal Data for the Permitted Purpose (as defined below) and to ensure that there are appropriate provisions and arrangements in place to properly safeguard the information shared between the Parties.

(C) As part of the collaborative arrangement to enable the provision of services, the parties have agreed to share Personal Data about potential participants.

NOW IT IS HEREBY AGREED as follows:

1. Definitions

1.1. The following terms shall have the meanings set out below.

1.1.1. **"Data Processing Particulars"** means, in relation to any processing: (a) the subject matter, duration, nature and purpose of the processing; (b) the type of Personal Data being processed; and (c) the categories of data subjects; as set out in more detail in Schedule One.

1.1.2. **“Supplier Personal Data”** means the Personal data to be collected by the Supplier from or in connection with the Customer Supplied Personal Data under this Agreement and further described in Schedule 1.

1.1.3. "**Data Protection Legislation**" means: (a) 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 is subject, including but not limited to the UK General Data Protection Regulation (“UK GDPR”), Data Protection Act 2018 ("DPA")

and the EU GDPR; and (b) any code of practice or guidance published by a Regulatory Body from time to time;

1.1.4. "**Data Subject Request**" means an actual or purported request, notice or complaint from (or on behalf of) a data subject exercising his rights under the Data Protection Legislation;

1.1.5. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

1.1.6. "**Participant/Respondent**" means any individual or organisation from or about whom data are collected;

1.1.7. "**Permitted Purpose**" means the purpose of the processing as set out in more detail in Schedule One (*Data Processing Particulars*);

1.1.8. "**Personal Data**" has the meaning set out in applicable Data Protection Legislation;

1.1.9. "**Personnel**" means all personnel involved in performing the Supplier's obligations under this Agreement from time to time (including its employees, staff, temporary staff, other workers, agents, consultants and its sub-contractors;

1.1.10. "**Regulatory Body**" means any competent governmental, statutory, regulatory or enforcement authority or regulator concerned with the activities carried on by any Party or any part, division or element thereof, in respect of the activities carried out pursuant to this Agreement including but not limited to the UK Information Commissioner, and their relevant successors (for the avoidance of doubt, this does not include any regulator whose authority arises pursuant to any voluntary code of conduct);

1.1.11. "**Regulatory Body Correspondence**" means any correspondence or communication (whether written or verbal) from a Regulatory Body;

1.1.12. "**Services**" means the Evaluation and Research Services the Supplier provides;

1.1.13. "**Customer Supplied Personal Data**" means the Personal data supplied by the Customer to be shared with the Supplier under this Agreement, as further described in Schedule 1.

1.1.14. "**Third Party Request**" means a written request from any third party for disclosure of Customer Data where compliance with such request is required or purported to be required by law or regulation;

1.1.15. "**Pseudonymisation**" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

1.1.16. "**UK GDPR**" means the UK data protection law that came into effect on 1st January 2021 to replace the EU GDPR and which will sit alongside the Data Protection Act 2018.

2. DATA PROTECTION

2.1. For the purposes of this Agreement, "**controller**", "**processor**", "**data subject**", "**Personal Data**" and "**process**" shall have the meanings set out in the UK GDPR and "**process**" and "**processed**" when used in relation to the processing of Customer's Data, will be construed accordingly, and will include both manual and automatic processing. Any reference to "**Personal Data**" includes a reference to "special categories of personal data", as applicable, whereby " special categories of personal data " means Customer's Data that incorporates such categories of data as are listed in Article 9(1) of the UK GDPR.

2.2. The Parties shall each process Personal Data under this Agreement. The Parties acknowledge that the factual arrangement between them dictates the classification of each Party in respect of the Data Protection Legislation. Notwithstanding the foregoing, the Parties anticipate that each Party shall act as a Controller in its own right as further set out in Schedule 1 (Data Processing Particulars.) For the avoidance of doubt, the parties are not joint controllers for the purposes of Article 26 of the UK GDPR.

2.3. In this sense, the Parties acknowledge and agree that:

2.3.1. Customer is acting as a Controller in its own right in relation to the Customer Supplied Personal Data that is processed by the Supplier, in the course of providing market and research services to Customer; and when the Supplier is collecting survey responses from respondents and/or Personal data in the course of providing the Services to Customer, the Supplier is acting as the Controller in its own right of survey responses and/or the collection of personal data which is not transferred back to the Customer unless otherwise agreed with participants' consent.

2.3.2. The Parties acknowledge that Personal Data provided to the Supplier will only be used for the purposes outlined in Schedule One (*Permitted Purpose*).

2.3.3. The Parties acknowledge that in the event of any conflict between the provisions of this Agreement and other agreements governing the processing of personal data, the provisions herein shall prevail.

2.3.4. Each of the Parties acknowledges and agrees that Schedule 1 (*Data Processing Particulars*) is an accurate description of the Data Processing Particulars.

2.3.5. Where a Party is acting as a Controller in relation to this Agreement, it shall comply with its obligations under the Data Protection Legislation and that Party shall ensure that it records due notification to any relevant Regulator, such notice to include its use and processing of the Personal Data.

2.3.6. Where the Supplier is acting as a processor in relation to this Agreement it shall:

2.3.6.1. comply with its obligations under the Data Protection Legislation.

2.3.6.2. process the Personal Data strictly in accordance with the Customer's instructions for the processing of the Customer Supplied Personal Data and only for the purposes of providing the Services or as otherwise instructed in writing by the Customer.

2.3.6.3. notify the Customer if it believes that any instruction issued by the Customer is not compliant with applicable Data Protection Legislation.

2.3.6.4. keep and maintain a record of processing as required under Article 30 (2) of the UK GDPR.

2.3.6.5. ensure that access to the Personal Data is limited to only those employees who require access to it for the purpose of providing the Services and that all such employees have undergone training in the law of data protection, their duty of confidentiality and in the care and handling of Personal Data.

2.3.6.6. assist the Customer promptly with all subject information requests which may be received from Data Subjects relating to the Customer Supplied Personal Data, as set out in Clause 2.12 and Clause 6.

2.3.6.7. employ appropriate operational and technological processes and procedures to keep the Personal Data safe from unauthorised use or access, loss, destruction, theft or disclosure, as set out in Clause 4.

2.3.6.8. not disclose the Personal Data to a third party in any circumstances other than at the specific written request of the Customer, unless the disclosure is required by law.

2.3.6.9. notify the Customer of any information security incident that may impact the processing of the Personal Data within 24 (twenty-four) hours of discovering or becoming aware of any such incident as set out in Clause 5.

2.3.6.10. not keep the Personal Data on any laptop or other removable drive or device unless that device is protected by being fully encrypted, and the use of the device or laptop is necessary for the provision of the Services.

2.3.7. Where a Party collects Personal Data which it subsequently transfers to the other Party, it shall:

2.3.7.1. ensure that it is not subject to any prohibition or restriction which would:

a. prevent or restrict it from disclosing or transferring the Personal Data to the other Party, as required under this Agreement; or

b. prevent or restrict the other Party from processing the Personal Data as envisaged under this Agreement;

2.3.7.2. ensure that all fair processing notices have been given (and/or, as applicable, valid consents obtained that have not been withdrawn) and are sufficient in scope and kept up-to-date in order to meet the Transparency Requirements to enable each Party to process the Personal Data in order to obtain the benefit of its rights, and to fulfil its obligations, under this Agreement in accordance with the Data Protection Legislation. For the avoidance of doubt, the Parties do not warrant to each other that any use of transferred Personal Data outside the scope of this Agreement shall be compliant with the Data Protection Legislation;

2.3.7.3. ensure that the Personal Data is:

a. adequate, relevant and limited to what is necessary in relation to the Permitted Purpose; and

b. accurate and, where necessary, up to date; having taking every reasonable step to ensure that any inaccurate Personal Data, (having regard to the Permitted Purpose), has been erased or rectified.

2.3.7.4. ensure that the Personal Data is transferred between the Parties by a secure means.

2.3.8. Each Party shall not, by its acts or omissions, cause the other Party to breach its respective obligations under the Data Protection Legislation, namely when one of the Parties has the duty to preserve the anonymity of the respondents.

2.3.9. Each Party shall indemnify and keep the other fully indemnified from and against any and all losses, fines, liabilities, damages, costs, claims, amounts paid in settlement and expenses (including legal fees, disbursements, costs of investigation, litigation, settlement, judgement, interest and penalties) that are sustained or suffered or incurred by, awarded against or agreed to be paid by, the other Party as a result of, or arising from, a breach by each Party of its obligations under this Clause 2 (*Data Protection*) and/or the Data Protection Legislation, including, in particular, pursuant to:

2.3.9.1. any monetary penalties or fines levied by any Regulatory Body on the other Party;

2.3.9.2. the costs of any investigative, corrective or compensatory action required by any Regulatory Body, or of defending proposed or actual enforcement taken by any Regulatory Body;

2.3.9.3. any losses suffered or incurred by, awarded against, or agreed to be paid by the other Party, pursuant to a claim, action or challenge made by a third party against the other Party, (including by a data subject); and

2.3.9.4. except to the extent covered by Clauses 2.10.1 or 2.10.2 or 2.10.3, any losses suffered or incurred, awarded against or agreed to be paid by the other Party.

2.3.10. Nothing in this Agreement will exclude, limit or restrict each Party's liability under the indemnity set out in Clause 2.10.

2.3.11. Where relevant, each Party shall notify the other promptly (and in any event within thirty-six (36) hours) following its receipt of any Data Subject Request or Regulatory Body Correspondence, which relates directly or indirectly to the processing of Personal Data under this Agreement or to either Party's compliance with the Data Protection Legislation, and together with such notices, or Regulatory Body Correspondence and reasonable details of circumstances giving rise to it. In addition to providing the notice referred to in this Clause 2.12, each Party shall:

2.3.11.1. only disclose such Personal Data in response to any Data Subject Request or Regulatory Body Correspondence where it has obtained the other party's prior written consent; and

2.3.11.2. provide the other Party with all reasonable cooperation and assistance required in relation to any such Data Subject Request or Regulatory Body Correspondence.

2.3.12. Notwithstanding the above, the parties acknowledge that the Supplier, in providing the services for the Project, is required to ensure participant anonymity. Accordingly, the Supplier shall provide to Customer's certain details of a Data Subject Request, without revealing the identity of the Data Subject. For the avoidance of doubt, the Supplier shall not be obliged to provide a copy of such Data Subject Request to Customer's.

2.3.13. The Supplier shall only disclose Personal Data to its Personnel that are required by the Supplier to assist it in meeting its obligations under this Agreement (the "**Project Personnel**") and shall ensure that no other Personnel shall have access to such Personal Data.

3. SUB-PROCESSING

3.1. For the purposes of this clause 3, the term "sub-processor" means any processor (as defined under the Data Protection Legislation) engaged by the Customer for carrying out specific processing activities in respect of any personal data supplied by the Supplier.

3.2. Where the Supplier is acting as a Processor, it may need to engage sub-processors. The Customer gives its general consent to Supplier's use of its sub-processors, as set out in Schedule Two *(List of Authorized Sub-processors).*

3.3. Where the Supplier engages sub-processors, the Supplier will enter into a contract with the sub-Processor that imposes on the sub-Processor the same obligations that apply to the Supplier under this Agreement.

3.4. Any sub-processing shall be strictly in accordance with the terms of this Agreement. Where the sub-processor fails to fulfil its data protection obligations, the Supplier will remain liable to the Customer for the performance of such sub-Processor's obligations.

4. SECURITY OF DATA PROCESSING

4.1. Each Party shall implement and maintain (in accordance with Article 32 of the UK GDPR appropriate technical and organisational measures, taking into account the state of the art, the implementation costs, and the nature, scope, circumstances and purpose of the processing, as well as the different probability of occurrence and the severity of the risk of the rights and freedoms of the persons concerned in order to ensure a level of protection appropriate to such risk. Such measures will include, but shall not be limited to:

4.1.1. the pseudonymisation and encryption of Personal Data, where appropriate;

4.1.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of relevant Processing systems and services;

4.1.3. the ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident, including a Personal Data Breach;

4.1.4. a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures in order to ensure the security of the Processing of Personal Data.

5. PERSONAL DATA BREACHES AND REPORTING PROCEDURES

5.1. The parties shall each comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) data subjects under Article 33 of the UK GDPR and, where applicable, shall each inform the other party without undue delay of any Personal Data Breach irrespective of whether there is a requirement to notify any Supervisory Authority or data subject(s).

5.2. When a Party is acting as a Processor, it shall notify the other Party immediately if it becomes aware of, or reasonably suspects the occurrence of, any potential or actual Personal Data Breach affecting Customer Supplied Personal Data and, in any event, within twenty-four (24) hours to enable the other Party to determine whether it must notify the Regulatory body in its own capacity as Controller.

5.3. The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.

6. DATA SUBJECTS' RIGHTS

6.1. The parties each agree to provide such assistance as is reasonably required to enable the other party to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation.

6.2. The parties shall notify each other as soon as reasonably practicable after becoming aware if they:

6.2.1. receive a request to rectify, block or erase any Personal Data;

6.2.2. receive any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation; or

6.2.3. becomes aware of a Data Loss Event.

6.2.4. The parties' obligations to notify under clause 6.2 shall include the provision of further information in phases, as details become available.

7. GOVERNING LAW AND JURISDICTION

7.1 This Agreement and any non-contractual obligations arising out of or in connection with it shall be governed by and interpreted in accordance with the laws of England and Wales.

7.2 Each Party irrevocably submits to the exclusive jurisdiction of the courts of England over any claim or matter arising under, or in connection with, this Agreement.

IN WITNESS WHEREOF, the Parties hereto have signed this Agreement as of the Effective Date. A duly authorised representative of each Party has read and understood this Agreement and hereby agrees to all its terms and conditions. Each person signing this Agreement warrants that he or she is duly authorised to do so and to bind the respective Party.

[insert DKG company name] **By: _____** **(Signature)** Name: _____ Title: _____	**[Customer]** **By: _____** **(Signature)** Name: _____ Title: _____

SCHEDULE 1

Data PROCESSING Particulars

Where the Parties are acting AS BOTH controllers IN THEIR OWN RIGHT

The subject matter and duration of the processing	
The nature and purpose of the processing	
The duration of the process	
The legal bases for processing the data processing	
The type of Personal Data being processed	
The categories of data subjects	
Permitted Purpose	
Data Protection Officer or when not applicable any other person acting as single point of contact on privacy or data protection matters	Data Protection Officer name For (Customer Org): (name and email address)

SCHEDULE TWO

List of authorized Sub-Processors

Company Name, corporate form and postal address	
Country	
Purpose	

Sub-Processor's Data Protection Officer contact information	

SCHEDULE THREE

DATA PROCESSING RESPONSIBILITIES

Activity	**Responsibility for making policy and decisions**	**Responsibility for implementing policy and decisions**
Lawful basis for processing of personal data [and of special categories of personal data] (Article[s] 6, 9 and 10)	Each party responsible for identifying its own legal basis in line with data protection legislation.	Each party will be responsible for deciding their own lawful basis
Purposes for which personal data may be collected (Article 5(1)(b))	[xx] will collect personal data for market research and analysis purposes only]	Each party will be responsible for ensuring they only process personal data for the agreed purpose.
Data minimisation (Article 5(1)(c))	Each party	Each party will be responsible for ensuring the personal data they collect and hold is no more than necessary for the purpose of the project.
Data accuracy (Article 5(1)(d))	Each party	Each party will be responsible for ensuring the personal data they collect and hold is accurate and kept up to date.
Data storage limitation (Article 5(1)(e))	Each party responsible for compliance in line with own policies and procedures	Each party responsible for compliance with data protection principles
Integrity and confidentiality (Article 5(1)(f))	Each party	Each party responsible for compliance with data protection principles
Accountability (Article 5(2))	Each party	Each party responsible for compliance with data protection principles
Information notices (Articles 13 and 14)	[to be determined, e.g.: [xx] shall issue the privacy notice identifying	Each party

	both parties as data controllers]	
Data subject rights (Articles 15 to 22)	Each party	Each party will be responsible for responding to requests from data subjects to exercise their rights in respect of the processing they undertake
Data protection by design and default (Article 25)	Each party	Each party
Appointment of Processor (Article 28)	Each party will appoint a processor if required, subject to other party's consent	Each party will do that independently
Records of processing activities (Article 30)	Each party shall keep separate records of processing activities in line with the main contract	Each party
Cooperation with supervisory authority (Article 31)	Each party will follow ICO's guidance/applicable guidance	Each party will follow ICO's guidance/applicable guidance
Security of processing (Article 32)	Each party	Each party has provided details about data security
Notification of data breach (Articles 33 and 34)	Each party shall inform the other about notifications of data breaches	Each party
Impact assessments (Articles 35 and 36)	[xx] if applicable (applicable when processing special categories of personal data and/or interviewing children/vulnerable people [please state N/A if not applicable]	[xx] shall provide details about their policy on Impact Assessments if applicable (applicable when processing special categories of personal data and/or interviewing children/vulnerable people [please state N/A if not applicable]