This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**") between

[DATA CONTROLLER NAME]

(the "**Company**")

and

Checkbox

(the "**Data Processor**")

(together as the "**Parties**")

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all Schedules;

1.1.2 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "**Contracted Processor**" means a Subprocessor;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.8 "**Data Transfer**" means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "**Services**" means the online questionnaire software and hosting services the Company provides.

1.1.10 "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data.

3. Processor Personnel

3.1 Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

3.2 Upon completion of the initial system setup and functional testing, the Processor shall remove Amazon Web Services (AWS) server and infrastructure access for all of Processor’s staff, except the Processor’s CEO. This is due to the technical constraints in the AWS account management system which does not allow for removal of all users. Access to the Checkbox software user interface shall be temporarily provided to a designated member of Processor’s staff for the limited purpose of assisting Company with its initial setup. No ongoing user accounts for Checkbox staff shall be retained.

3.3 Neither the CEO nor any other individual at the Processor shall access Company data except with prior written permission from the Company for troubleshooting or support purposes.

4. Security

4.1 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, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In determining the appropriate level of security, the Processor shall duly consider the risks inherent in the Processing of Personal Data, with particular regard to the likelihood and severity of a potential Personal Data Breach.

4.3 The Processor shall implement and maintain private servers dedicated exclusively for use by the Company on Amazon Web Services.

4.4 All servers operated by the Processor for Company data shall be located in [EU HOSTING COUNTRY], ensuring all data remains within the European Union.

4.5 No other applications, save for the Processor's application deployed for the Company, shall operate on these dedicated servers.

4.6 All data relating to the Company shall remain in the private AWS environment under the Processor's control, including all backups and security logs. No data will be stored outside of this secure environment.

4.7 The Processor shall not export any data outside of the AWS environment except when necessary to export logs for internal investigation related to security incidents. Such log exports shall be handled solely by the Processor and shall not be shared with any third-party data processors.

5. Subprocessing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by the Company.

5.2 The Processor engages Amazon Web Services (AWS) as a Subprocessor to host and manage the infrastructure used to process Company Personal Data. AWS provides infrastructure-as-a-service and does not access or process the data for any other purpose. AWS is bound by a separate Data Processing Addendum (DPA) that details the technical and organizational security measures AWS implements in compliance with GDPR requirements. The Processor remains fully responsible for AWS’s compliance with these obligations under this Agreement.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, where applicable, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws. In general, Survey responses are anonymous and the Processor does not have the ability to link survey responses to individual responses. Therefore, in case the response cannot be linked to an individual, the Processor cannot fulfill requests to access, correct, or delete individual responses.

6.2 In the event that data appears to be identifiable, Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws, inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay, but no later than 24 hours, upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.3 In the event of a Personal Data Breach involving identifiable data, the Processor shall take the following steps :

7.3.1 Contain the Breach: Take immediate action to limit exposure and prevent additional data loss. This might include shutting down affected systems, revoking access, or isolating compromised environments.

7.3.2 Assess the Risks: Investigate the incident's scope, affected data, and potential harm to individuals. Review whether sensitive data was involved and the encryption or security measures in place.

7.3.3 The Processor shall notify the Required Parties:

a) If the breach poses a risk to data subjects' rights and freedoms, notify the [COMPETENT SUPERVISORY AUTHORITY] within the legally required time frame of 72 hours.

b) If there is a high risk to individuals, inform the data controller ([DATA CONTROLLER NAME]) of the affected data subjects so they can inform the subjects directly. Notification details typically include the breach nature, affected data, planned mitigation steps, and contact for further questions.

7.3.4 Document the Incident: Record the breach details, response steps taken, and decisions made. Maintain these records for regulatory audits and legal compliance.

7.3.5 Review and Prevent Recurrence: After containment and notification, conduct a post-incident analysis to identify lessons learned and improve security controls based on findings.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in

relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1 Upon closure of the Company's questionnaire and completion of the requisite export of the data by the Company for its records and use, the Processor shall schedule the permanent deletion of all associated data in consultation with the Company.

9.2 Processor shall provide written certification to Company that it has fully complied with this section 9.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. Liability

The Processor shall be liable to the Controller for any damages (including, but not limited to, fines imposed by the supervisory authority directly attributable to Processor's proven breach) directly resulting from its proven breach of obligations specifically assigned to it under this Data Processing Agreement or any applicable data protection laws, including the GDPR. The Processor shall indemnify and hold harmless the Controller from all claims by third parties, damages, costs, or other expenses resulting therefrom to the extent that such claims directly result from Processor's proven breach of this Agreement or any applicable data protection laws. Only direct damages shall be eligible for compensation; liability for indirect damages, including consequential damages, lost profits, missed savings, and damages due to business interruption, is excluded. This limitation does not apply in cases of willful misconduct or gross negligence by the Processor's management. Processor's total aggregate liability shall be capped at 2 (two) times the annual fees paid or payable by the Controller under this Agreement in the preceding twelve (12) months. If any overarching liability provisions exist in other agreements between the parties, the liability provisions set forth in this Data Processing Agreement (DPA) shall prevail and govern with respect to the matters covered herein.

13. General Terms

13.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“Confidential Information”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

13.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

14. Governing Law and Jurisdiction

14.1 This Agreement is governed by the laws of the State of Delaware, United States of America.

14.2 Any disputes arising out of this Agreement shall be resolved through arbitration in the state of Delaware under the rules of the Delaware Rapid Arbitration Act (DRAA).

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Your Company

Signature _____

Name: _____

Title: _____

Date Signed: _____

Processor Company

Signature _____

Name: _____

Title: _____

Date Signed: _____

Schedule 1: Overview of the types of Personal Data processing and of the purposes of processing

The information below shall be provided whenever a Data Processing Agreement is concluded. It gives a full overview of the Personal Data that will be processed. This makes it easier to prove where, by whom and for which purposes the Personal Data are processed.

Description of processing activities by the Data Processor	Storage of data (answers to questionnaires) on dedicated server and ensure access by controller to the server
Purposes of processing	[PURPOSES OF PROCESSING]
Categories of personal data	In most cases the data in the questionnaire will be anonymous. However, it may be possible that the questionnaire entails personal data. In that case, the questionnaire can include: [CATEGORIES OF PERSONAL DATA, e.g. e-mail, name, surname] [SPECIAL CATEGORIES OF PERSONAL DATA / CRIMINAL CONVICTIONS AND OFFENCES DATA, IF ANY]
Categories of data subjects	[CATEGORIES OF DATA SUBJECTS]
Data Controller	[DATA CONTROLLER NAME]
Data Processor	Checkbox
Sub Data Processors	AWS
Place of processing	[PLACE(S) OF PROCESSING], [EU HOSTING COUNTRY]
Retention period	After the contract in agreement with the Company

Schedule 2: Technical and organizational measures

Technical Measures	All network traffic entering and leaving the private server is protected with SSL encryption. Additionally, the Microsoft SQL Server database is encrypted using Transparent data encryption (TDE).
Organizational Measures	Except for the Processor’s CEO, all access to Accounts and Data by the Processor’s personnel shall be terminated immediately upon completion of the account setup on the private AWS server, as further specified in Section 3.