Data & Privacy Protection Service Agreement

The purpose of the clauses stated in this agreement is to define the conditions under which the **Service Provider** [**Globibo Pte Ltd**] undertakes to carry out the personal data processing operations defined below on behalf of the **Customer** [**.....**].
As part of their contractual relationship, the parties undertake to comply with the regulations in effect applicable to personal data processing and privacy in general and local policies in specific countries. Under the terms of this agreement, the following terms are defined as follows:

- "PDPPP": legislation and government policies applicable in the country in regards to Personal Data and Privacy Protection Policies
- "Customer": the organization that engages another organization (Service Provider) to provide services relating to the processing of personal data (such as hosting or storage of data, payroll processing, event & registration information, etc.)
- "Service Provider": the organization that provides the service of processing personal data on behalf of, and for the purposes of, a Customer will likely be considered as a data intermediary of the Customer under the applicable PDPPP
- "Personal Data": data, whether true or not, about an individual who can be identified
    - from that data alone; or
    - from that data and other information which the Service Provider has or is likely to have access
- "Customer Personal Data": personal data which the Customer discloses to the Service Provider, or which the Service Provider processes on behalf of the Customer.

1. Data Protection Clauses

A. Compliance with PDPPP

- The Service Provider shall comply with all its obligations under the PDPPP at its own cost.
- The Service Provider undertakes to take into account of data protection principles and data protection by default from the design stage onwards of tools, products, applications and services.
- The Service Provider shall cooperate with the Customer and use its best endeavors to help the Customer prove that it is compliant with all its legislative and regulatory obligations, notably in respect of the PDPPP.
- In particular, the Service Provider shall, where relevant, assist the Customer with carrying out impact analyses in respect of data protection and also assist the Customer in carrying out a prior consultation with the regulatory authority.
- If the Service Provider considers an instruction constitutes an infringement of the PDPPP, or any other law on data protection, it must inform the Customer immediately.

B. Documentation

- The Service Provider shall provide the Customer with specific documentation required to demonstrate compliance with all its obligations and to enable audits and inspections to be carried out by the Customer or another auditor appointed by it, and to contribute to said audits.

C. Process, Use and Disclosure

The Service Provider shall only process, use or disclose Customer Personal Data:

- strictly for the purpose of survey respondents' data collection and retention in system hosted by the Service Provider under this agreement;
- with the Customer's prior written consent ; or
- when required by law or an order of court, but shall notify the Customer as soon as practicable before complying with such law or order of court at its own costs.

D. Confidentiality of Customer Personal Data

- The Service Provider shall ensure the confidentiality of Customer Personal Data processed under this agreement.
- The Service Provider ensure that those authorized are to treat Customer Personal Data according to this agreement:

    A. undertake to respect confidentiality, or are to subject to an appropriate statutory confidentiality obligation,
    B. receive the necessary training in respect of Customer Personal Data & Privacy protection.

E. Transfer of Data

- The Service Provider undertakes not to disclose, make accessible or transfer any of the Customer Personal Data, even for routing purposes, except with the Customer's prior written consent.
- The Customer reserves the right to carry out any checks it deems necessary to confirm the performance of the obligations arising under this clause.

- The Service Provider reserves the right to deploy backup services and / or utilize server infrastructures, for the primary operation of the system only, that include geographically distributed file storage, including, but not limited to, Microsoft Azure and Amazon Web Services and Google Servers. A list of utilized partner can be provided to the Customer upon request at any time.

F. Security Measures

- The Service Provider acknowledges that security is a fundamental criterion for the Customer and that the Service Provider's compliance with the security requirements defined in the schedule to this agreement is an essential and decisive obligation for the Customer's consent thereto.
- The Service Provider shall protect Customer Personal Data in the Service Provider's control or possession by making reasonable security arrangements (including, where appropriate, physical, administrative, procedural, and information & communications technology measures) to prevent unauthorized or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of Customer Personal Data, or other similar risks.
- The Service Provider shall only permit authorized personnel to access Customer Personal Data on a need to know basis.

G. Access to Personal Data

- The Service Provider shall provide the Customer with access to the Customer Personal Data that the Service Provider had in its possession or control, as soon as practicable upon Customer's written request.
- In the event that the Customer authorises the Service Provider to this effect, it will be the latter's responsibility to provide information relating to the data processing carried out by it to the data subjects concerned by the processing operations at the time the data are collected. The formulation and format of the information must be agreed with the Customer before the data are collected.

H. Accuracy and Correction of Personal Data

- Where the Customer provides Customer Personal Data to the Service Provider, the Customer shall make reasonable effort to ensure that the Customer Personal Data is accurate and complete before providing the same to the Service Provider.
- The Service Provider shall put in place adequate measures to ensure that the Customer Personal Data in its possession or control remain or is otherwise accurate and complete. In any case, the Service Provider shall take steps to correct any errors in the Customer Personal Data, as soon as practicable upon the Customer's written request.

I. Retention of Personal Data

- The Service Provider shall not retain Customer Personal Data (or any documents or records containing Customer Personal Data, electronic or otherwise) for any period of time longer than 15 calendar days upon Customer's written request to serve the purpose of this agreement.
- The Service Provider shall, upon the request of the Customer:
  A. return to the Customer, all Customer Personal Data; or
  B. delete all Customer Personal Data in its possession,
  C. and, after returning or deleting all Customer Personal Data, provide the Customer with written confirmation that it no longer possesses any Customer Personal Data.
- Where applicable, the Service Provider shall also instruct all third parties to whom it has disclosed Customer Personal Data for the purposes of this agreement to return to the Service Provider or delete, such Customer Personal Data.
- The return of all files, data, programs, documentation etc. is included in the price for the provision of service.
- The Service Provider must confirm the actual destruction of the Customer Personal Data within 15 calendar days of the Customer's request or the end of the agreement.
- This clause will remain in effect after the expiry or termination of the Quotation contract for any reason whatsoever.

J. Notification of Breach

- The Service Provider must notify the Customer of any Customer Personal Data breach within 48 hours after becoming aware of it, by email to the project manager of the Customer.
- The Service Provider must, throughout the period of the agreement, set up and maintain a process and procedures to manage security incidents (including, in particular, breaches of personal data) and ensure continuity of service in accordance with industry standards.
- The Service Provider shall notify the Customer of the name and contact details of one of its employees, who shall act as the Customer's primary point of contact in respect of security issues. Any request from the Customer relating to security must be treated diligently and as a priority by the Service Provider.
- Without prejudice to the Customer's other rights and remedies, in the event of a presumed or proven security incident or breach of personal data, the Service Provider must advise the Customer immediately and at the latest, within 48 hours following the occurrence of the security incident or breach of personal data.

- Immediately after said notification, the Parties will coordinate their actions in order to investigate the security incident concerned. The Service Provider undertakes to cooperate fully with the Customer, at its own expense, to help it to manage the situation, including but not limited to:
  A. helping it with any investigation;
  B. providing the Customer or an independent third party appointed by the Customer with physical access to the facilities and operations concerned;
  C. organizing interviews with the employees of the Customer and all other appropriate individuals; and
  D. providing all registers, logs, files, data communications and other relevant documents necessary for compliance with laws, regulations and industry standards.
- The Service Provider will also provide all reasonable assistance to the Customer in the case of a notification in respect of any action the latter may be obliged or may choose to take in respect of a personal data breach.
- The Service Provider undertakes not to inform third parties, including the persons concerned, of any breach of Customer Personal Data without having obtained the prior consent of the Customer in writing, except in the cases provided for in the PDPPP.
- Moreover, the Service Provider acknowledges that the Customer has sole authority to determine:
  A. whether or not the breach of Customer Personal Data must be notified to any individual, regulatory authority, administrative authority or other person pursuant to the PDPPP; and
  B. the content of said notification.
- The Service Provider shall take the appropriate measures, at its own expense, to mitigate the consequences of any security incident and remedy it, and shall make all the amendments it judges necessary in order to avoid any reoccurrence of an incident of this kind. The Service Provider shall assist the Customer, at its own expense, with restoring, if technically and commercially viable, the Customer's data in the event of a Customer Personal Data loss caused by any failure to fulfil its regulations in respect of the Contract.
- The Service Provider shall cooperate and provide the Customer with the necessary assistance in respect of any complaint formulated by a data subject or any investigation or request issued by a regulatory authority with regard to the PDPPP or any other applicable regulation.
- The Service Provider shall maintain a record of security incidents and make this available to the Customer, including but not limited to breaches of Customer Personal Data, and shall document all relevant information concerning the circumstances of said incidents and breaches, the harm caused and corrective measures taken to mitigate their effects, as well as the actions and measures taken to avoid any repetition of such incidents or breaches. Those records are made available within the premises of the Service Provider upon prior notice and jointly agreed timeframe.

K. Indemnity

The Service Provider shall indemnify the Customer and its officers, employees and agents, against all actions, claims, demands, losses, damages, statutory penalties, expenses and cost (including legal costs on an indemnity basis), in respect of:

- the Service Provider's breach of clauses stated; or
- any act, omission or negligence of the Service Provider or Subservice Provider that causes or results in the Customer being in breach of the PDPPA.

2. Customer's obligations in respect of the Service Provider

The Customer undertakes, throughout the term of the agreement, to:

- document in writing any additional instructions regarding the processing of data by the Service Provider;
- ensure, prior to and during the period of processing, compliance with the obligations set out in Data Protection Policies by the Service Provider;
- supervise the processing, including carrying out audits and inspections at the Service Provider's premises in accordance with the provisions of this agreement.

3. Exercise of individual rights

So far as possible, the Service Provider must help the Customer to fulfil its obligation to respond to requests to exercise their rights by data subjects, including rights of access, correction, deletion and opposition, right to restriction of processing, right to data portability and right not to be the subject to an automated individual decision (including profiling).
Should the persons concerned make a request to exercise their rights to the Service Provider, said Service Provider must send such requests, on receipt, in writing to the Customer's project manager.

4. Subcontracting

The Service Provider may call on another Service Provider (hereinafter "the subsequent Service Provider") to carry out specific processing activities. In this case, the Service Provider must inform the Customer in advance, and in writing, of any planned changes with regards to adding or replacing other Service Providers. This information must clearly indicate the processing activities subcontracted, identity and contact details of the Service Provider and the dates of the subcontracting agreement. The Customer has a minimum period of one (1) month from the date of receipt of said information to present its objections. Said subcontracting may only proceed if the Customer has not expressed an objection during the agreed period. Server hosts and backup services from Microsoft Azure, Amazon and Google cloud do not require such prior approval.

The subsequent Service Provider is obliged to fulfil the obligations set out in this agreement on behalf of the Customer and in accordance with their instructions. It is the initial Service Provider's responsibility to ensure that the subsequent Service Provider offers the same sufficient guarantees in respect of the implementation of appropriate technical and organizational measures to ensure that the processing meets the requirements of the Data & Privacy Protection Policies. Should the subsequent Service Provider fail to fulfil their obligations in respect of data protection, the initial Service Provider shall retain full responsibility in respect of the Customer for the other Service Provider's fulfilment of its obligations.

5. Audit

Throughout the term of the agreement, the Customer may carry out tests and audits of all or some of the services, either by itself or through an independent third party at its expenses - subject to five (5) working days' prior notice -, in order to ensure compliance with the stipulations of the contract in terms of:

- Compliance with security policies,
- Quality of services, in particular to ensure the integrity and confidentiality of the Customer's data

Where the services involve the processing of personal data, the audit may also relate to the verification of PDPPP and the verification of:

- locations used for the processing and/storage of personal data;
- measures taken to ensure the security of personal data and combat breaches of personal data.

The Service Provider undertakes to authorize the Customer, or companies appointed by the latter and tasked with carrying out the audit, to access the necessary information to carry out their audit properly and, if possible, access the sites where the services are delivered.

The Service Provider will cooperate fully (and, where Service Provider and representatives are concerned, ensure their cooperation) with the Customer and, depending on the case, the audit representatives of the Customer, including giving them access to the premises, personnel, physical and technical environments, equipment, software, documentation, data, registers and systems relating to the services, and any useful information that might reasonably be necessary in carrying out the audit.

An audit report must be sent to the Service Provider. Should it become apparent, following the audit and testing measures described above, that the security measures implemented by the Service Provider are not appropriate or sufficient, or if said audits or tests reveal any gaps or examples of non-compliance with the requirements set out in this Contract and/or the legal requirements applicable and/or the standards in effect, the processor will implement corrective actions within a time frame to be agreed between the Parties, depending on the severity of the failure observed and in any case.

6. Effect of agreement and changes to agreement

This agreement applies in conjunction with any other agreements, contractual clauses and consent clauses that apply in relation to the collection, use and disclosure of the personal data by the Service Provider.

ACKNOWLEDGEMENT AND CONSENT

Customer - <details go here>	Service Provider - Globibo Pte Ltd
Date: Name: Signature:	Date: Name: Signature: