SurveySparrow

Data Processing Addendum

Legal | Effective Date : 27th December 2022

This Data Processing Addendum ("DPA" or "Addendum") is incorporated into and subject to the SurveySparrow Terms of Service located at https://surveysparrow.com/legal/terms-of-service/ (otherwise known as "Service Agreement" or "Agreement") and entered into between SurveySparrow Inc. including its Affiliates and the Customer. This Addendum has been entered to ensure utmost privacy, security and data protection in compliance with the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 - 1798.199) ("CCPA"), the UK General Data Protection Regulation where applicable. For the avoidance of doubt, it is hereby clarified that this Addendum together with its Exhibits and Annexures (collectively, the "DPA") specify the obligation of the Parties when SurveySparrow is acting in the capacity of Processor, as defined below.

This Addendum is supplemental to, and forms an integral part of the Agreement and becomes effective and binding upon entering into the Service Agreement as applicable, the details of which may be specified in the Agreement, an Order Form or an executed version or its amendment to the Agreement. In case of any conflict or inconsistency with the Service Agreement and the DPA, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency with respect to the subject matter at conflict.

1. DEFINITIONS

Capitalized terms used but not defined in this Addendum shall either have the same meaning as set forth in Article 4 of the GDPR or the Service Agreement as applicable.

"Customer" means the person or entity placing an order for or accessing the Service under the Service Agreement.

"Customer Data" means all data (including but not limited to Customer Personal Data and End User data uploaded to or created on SurveySparrow platform) that SurveySparrow in its

capacity as Data Processor processes on behalf of the Data Controller through the provision of its Services.

"**Data**" or "**Personal Data**"means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with identified or identifiable natural person or Consumer (as defined in the CCPA) which is processed solely by SurveySparrow , on behalf of the Customer for the purpose of delivering Services.

"**Data Controller**" or "**Controller**" or "**Data Exporter**" means the Customer entity who collects Personal Data and uses the Services of SurveySparrow . either free or under paid subscription model who determines the purposes and means of the Processing of Personal Data;

"**Data Processor**" or "**Processor**" or "**Data Importer**" means SurveySparrow Inc. who processes Personal Data on behalf of the Data Controller under its Instructions.

"**Data Protection Officer**" means the designated representative of the Parties who will be the point of contact for any Data Privacy/Security related issues/queries;

"**Data Subject"** means the individual to whom Personal Data relates.

"**Data Protection Laws**" or **"Regulations"** means all data protection laws and regulations applicable to a party's processing of Customer Data under the Agreement, including, where applicable, the EU Data Protection Directive 95/46/EC, the Privacy and Electronic Communications Directive 2002/58/EC and the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the GDPR as it forms part of UK law by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (all of which are as may be amended from time to time);

"EEA" means, for the purpose of this Addendum, the European Economic Area;

"**Instruction**" means the written, documented instruction, issued by the Controller to the Processor, requesting Processor to perform a specific action on the Personal Data (including, but not limited to, updating, blocking, deleting, depersonalizing, transferring);

"**Personal Data Breach**" means a security incident, leading to the accidental or unlawful destruction, loss, alteration, unauthorized divulgence, or access to, Personal Data transmitted, stored or otherwise processed by us and/or our Sub-Processors in connection with the provision of Services under the Terms of Services;

"**Processing"** shall mean any operation or set of operations which is performed upon Personal Data whether or not by automatic means, including collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Personal Data as defined in the applicable data privacy laws.

"**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"**Services**" means the services agreed to be provided by Data Processor to the Data Controller under the Terms of Service in relation to the proprietary online survey application viz. 'SurveySparrow' owned by the Data Processor, including hosting of such application on cloud server, providing access to authorised users of the Customer, trouble shooting related services, consultancy and customer support services on request;

"**Standard Contractual Clauses**" means in relation to the EEA, the contractual terms approved under the European Commission's decision of 4 June 2021 on Standard Contractual Clauses (Commission Decision (EU) 2021/914) for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679;

"**Sub-processor**" or "**Sub-data Processor**" means the third party service providers engaged by the Data Processor who interact with the Controller's Data (in part or full) so as to assist the Data Processor in fulfilling its obligations with respect to providing the Services as per the Terms of Service.

"**Supervisory Authority**" means any competent regulatory authority including data protection authorities and law enforcement agencies.

"**UK Addendum**" means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 found at https://ico.org.uk/media/about-the-ico/consultations/2620398/draft-ico-addendum-to-com-scc-20210805.pdf

2. INTRODUCTION

- The terms of this Agreement shall apply to the extent Personal Data is provided to Processor or the Processor is exposed to while providing Services.
- To the extent of Processing of Personal Data pursuant to this Addendum, SurveySparrow Inc. shall be the Data Processor and customer shall act as the Data Controller.
- The terms of this Addendum shall apply to the extent such Personal Data is provided to the Processor or the Processor is exposed to, while providing the Services.
- The Data Controller is responsible for providing the Processor access only to such Personal Data as needed for the performance of the Services and as may subsequently be agreed in writing by the parties, in which case the Data Processor shall act solely under such documented instructions from the Data Controller. And the parties further agree that this Addendum together with Service Agreement, documents incorporated by reference including Order Form constitutes such written instructions of the Controller to process Customer Personal Data (including but not limited to locations outside of the EEA and UK) along with other reasonable written instructions provided from time to time by the Customer (e.g. email communications) where such instructions are consistent with the Addendum;

3. DETAILS OF PROCESSING OF PERSONAL DATA

- **Data Subjects**: means the identified or identifiable person to whom the Personal Data relates to and includes Data Controller's employees, contractors, customers, prospects, suppliers and subcontractors.

- **Personal Data**: This includes contact information, the extent of which is determined and controlled by the Customer in its sole discretion, and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by end users via the Services.

- **Nature of the Processing**: The subject-matter of Processing of Personal Data by Data Processor is the provision of the Services to the Data Controller that involves the Processing of Personal Data, as specified in the Terms of Service.

- **Purpose of the Processing**: Personal Data will be Processed for purposes of providing the Services set out in the Terms of Service.

- **Duration of the Processing**: Personal Data will be Processed for the duration of the provision of Services under the Terms of Service or Service Order as the case may be, including its renewal , subject to Clause 8 of this Addendum.

4. DATA PROCESSOR OBLIGATION

The Data Processor agrees to process the Data only in accordance with relevant data protection laws and in particular on the following conditions:

4.1. Data Processing:

The Data Processor shall only process Personal Data in accordance with the Data Protection Legislation and according to Instructions from the Data Controller and solely for the Services promised to the Data Controller, and not for its own, independent

purposes. The Data Controller has the right to access, modify, delete and transfer their Personal Data.

Data Processor shall not itself exercise control, nor shall it transfer, or purport to transfer, control of such Personal Data to a third party, except as it may be specifically instructed by the Controller.

The Data Processor shall be obliged to perform appropriate technical and organizational measures in such a way that the data processing meets the requirements of the legislation in force at any time and ensures protection of the rights of the Data Subject(s).

The Data Processor will be responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data and the Processing of Personal Data.

The Data Processor will make available information necessary for the Data Controller to demonstrate compliance with the GDPR (Article 28 obligations) where such information is in the control and possession of the Data Processor and is not otherwise available to the Data Controller through its account or on Data Processor website, provided that the Data Controller provides the Data Processor with at least 14 (fourteen) days' written notice of such an information request.

The Data Processor is prohibited from selling Personal Data. No Personal Data shall be disclosed/transferred to any third-parties in a manner that would suggest “selling” under applicable law, i.e., CCPA.

4.2. Confidentiality:

The Data Processor shall be obliged to ensure that the persons authorized to process Personal Data have contractually committed to confidentiality obligations or are subject to an appropriate statutory duty of confidentiality.

4.3. Sub- Processor

By entering into this Addendum, the Data Controller authorizes the use of Sub-Processor(s) by the Data Processor for the provision of Services as agreed under the Terms of Service. The Data Processor will make available to the Data Controller, the list of Sub-processors engaged by it for the provision of Services to the Data Controller, together with the description of the nature of services and data center location of each such sub-processorThe current list of Sub-processors is provided in Annexure III. The Data Processor will notify the Data Controller via email in case of new additions to the list, if any. However, the Data Controller can refer to the said Annexure of this DPA from time to time, in case they have opted out of the Processor's email notification.

Upon such notification by the Data Processor, the Data Controller may, on legitimate grounds, object to the addition or replacement of Sub-processor, by notifying SurveySparrow Inc. promptly in writing an email to privacy@surveysparrow.com within ten (10) Business Days after receipt of the Data Processor's email notice. The following terms shall apply in the event Data Processor notifies the Data Controller of addition or replacement of Sub-processor:

1. If the Data Controller objects to such addition or replacement of the Sub-processor on any reasonable grounds, it shall be notified to the Data Processor in writing. The parties shall discuss such concerns in good faith with a view to achieve a commercially reasonable and technically viable resolution. If the Data Processor is unable to consider Controller's objection and no such resolution can be reached and the same being notified to the Controller, the Controller may as its sole remedy, terminate the subscription for the affected service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval.

2. If the affected service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite.

3. No amounts shall be refunded by the Data Processor to the Controller.

Where SurveySparrow engages Sub-Processors as set forth herein, it shall ensure that such sub-processors are contractually bound to provide at least the same level of protection for Personal Data as those contained in this Addendum including, wherever applicable, the Standard Contractual Clauses) to the extent applicable to the nature of services provided by such sub-processors. In any event we shall remain responsible for sub-processors compliance with this DPA and liable for all acts and omissions of such sub-processors that cause SurveySparrow to breach any of its obligations contained in this Addendum.

4.4. Audits

The Data Processor will ensure the availability of a "Data Protection Officer" who will be incharge of the Data security and whom the Data Controller can approach by sending an email to privacy@surveysparrow.com in case of any queries relating to their Data.

The Data Controller may, prior to the commencement of Processing, and at regular intervals, audit the technical and organizational measures taken by SurveySparrow Inc. as a Processor and for such purposes, the Data Controller may:

1. obtain relevant information from the Processor necessary to demonstrate compliance with this DPA,

2. request the Processor to submit to the Controller an existing attestation or certificate by an independent professional expert, or

3. upon fifteen (15) days' prior written request at reasonable intervals (not more than once in 12 months) , during regular business hours and without interrupting Processor's business operations, conduct audit including an on-site inspection of Processor's business operations or have the same conducted by a qualified third party which shall not be a competitor of the Processor directly or indirectly and such third party shall enter into appropriate confidentiality agreements with Processor.

Upon receiving the written request from the Data Controller, the Data Processor will provide with all information necessary for such audit (provided, however, that such information, audits, inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by the Data Controller to assess in compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Processor's prior written approval), to the extent that such information is within the Processor's control. Provided, the Controller bears any and all cost involved for conducting the same. And further upon Processor's first request, the Data Controller shall return all records or documentation in Data Controller's possession or control provided by Processor in the context of the audit and/or the inspection).

4.5. Request from Data Subjects

To the extent that Data Controller is unable to respond to Data Subject request without the aid and support of the Data Processor, the Processor upon request of the Data Controller in writing will make available , Personal Data of Data Subjects and support the Controller to fulfill requests by Data Subjects to exercise their rights under the GDPR in a manner consistent with the functionality of the software product and SurveySparrow's role as a Processor. SurveySparrow shall comply with reasonable requests of the Controller and in return Controller agrees to reimburse SurveySparrow for such assistance.

If SurveySparrow receives a request from the Data Subject to exercise its rights under the GDPR, SurveySparrow will redirect such Data Subject to the Controller. The Controller shall be solely responsible for timely response to any such Data Subject Requests or communications involving Personal Data.

4.6. Security

The Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, as described under Appendix 2 of the Standard Contractual Clauses. Such measures include, but are not be limited to:

- the prevention of unauthorized persons from gaining access to Personal Data Processing systems (physical access control),
- the prevention of Personal Data Processing systems from being used without authorization (logical access control),
- ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control),
- ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),
- ensuring the establishment of an audit trail to document whether and by whom Personal Data has been entered into, modified in, or removed from Personal Data Processing systems (entry control),
- ensuring that Personal Data is Processed solely in accordance with the Instructions (control of instructions),
- ensuring that Personal Data is protected against accidental destruction or loss (availability control).

Notwithstanding any provision to the contrary, Data Processor may modify or update the Security Measures at its discretion for legitimate reasons; provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

5. DATA CONTROLLER OBLIGATION

The Data Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data. The Data Controller:

- represents and warrants to comply with the terms of this Addendum, and all applicable data protection laws.
- represents and warrants that any and all necessary permissions and authorizations have been obtained, necessary to permit SurveySparrow Inc., its affiliates and Sub-Processors, to execute their rights or perform their obligations in connection with processing of Personal Data under this Addendum.
- Agrees to be responsible for compliance with all applicable data protection legislation, including requirements with regards to the transfer of Personal Data under this Addendum.
- Shall have the sole responsibility for the accuracy, quality, and legality of Personal Data collected and the means by which Controller acquired such Personal Data of its customer.
- ensures that its Instructions to the Data Processor regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws;
- Represents and warrants that it has the right to transfer, or provide access to, the Personal Data to the Data Processor for Processing in accordance with the terms of this Addendum and Terms of Service.

- Agrees to ensure that all affiliates of the Data Controller who use the Services shall comply with the obligations set out in this Addendum.

6. PERSONAL DATA BREACH

The Data Processor will promptly, and without any undue delay, notify the Data Controller within 48 hours after becoming aware of a security incident, so long as applicable law allows this notice. The Data Processor to the extent permitted and required by Data Protection Laws shall provide timely information relating to the security incident involving the Data Controller's Personal Data.

Neither the Data Controller nor the Data Processor shall be deemed liable to the other Party for any circumstances beyond the control of the Party, which the Party upon entering this Addendum could not have taken into consideration, avoided or overcome.

7. INTERNATIONAL TRANSFER OF DATA

SurveySparrow Inc., may transfer Personal Data to the United States and/or to other third countries where SurveySparrow Inc., or its Sub-processors operate for purposes of offering the services, the details of which can be obtained as stated in Section 4.3. SurveySparrow Inc. will follow the requirements of this Addendum regardless of where such Personal Data is stored or processed. Wherever there is a Restricted Transfer of Personal Data, SurveySparrow will ensure such transfers are made in compliance with the requirements of Data Protection Laws and in accordance with this Addendum.

SurveySparrow will not transfer Personal Data that is subject to the European data protection law to any country or recipient not recognized as providing an adequate level of protection for Personal Data without taking all such measures as are necessary to ensure the transfer is in compliance with applicable European data protection laws. Such measures include Standard Contractual Clauses, implementation of security, technical and organizational measures as detailed in Appendix 2 to the SCC.

In relation to the processing of Personal Data that is subject to the UK GDPR, the Standard Contractual Clauses will be modified and interpreted in accordance with the UK Addendum

which shall be deemed to be incorporated by reference and forms an integral part of this Addendum. For the sake of clarity, Tables 1, 2 and 3 of the UK Addendum will be deemed completed with the information set out in the Annexes of this DPA and Table 4 will be deemed completed by selecting “neither party”; and any conflict between the terms of the Standard Contractual Clauses and the UK Addendum will be resolved in accordance with Section 10 and 11 of the UK Addendum.

8. TERM & TERMINATION OF THIS ADDENDUM

This Addendum shall remain valid, effective and binding on the Parties until the sooner termination or expiration of Services under the terms of Service.

The Addendum will automatically stand terminated with effect due to discontinuance of Services between the two parties, either due to non-renewal or cancellation of Services Agreement.

9. DELETION OR RETURN OF CUSTOMER DATA

Upon termination or expiration of the Agreement, the Data Processor shall, no later than 30 days, at the request of the Data Controller either delete or return the Customer Data (including its copies, if any) that is in its possession or control and Processed under this Addendum as set out in the Privacy Policy except that are required by applicable law to retain either in whole or in part, or otherwise that are archived on back up systems which the Data Processor shall securely isolate, protect from any further processing and eventually delete in accordance with this DPA.

9. MISCELLANEOUS

The term Addendum means and includes this document and the annexes, exhibits referred to herein and all amendments thereto. If any term, condition, section or provision of this Addendum becomes invalid or be so judged, the remaining terms, conditions, sections and provisions shall be deemed severable and shall remain in force. The failure to exercise, or

delay in exercising any right, power or remedy vested in this Addendumshall not constitute a waiver by that party of that or any other right, power or remedy. The Data Processor reserves the right, at its sole discretion, to amend the DPA to reflect the technical, organisational and regulatory requirements and any change in the terms contained herein shall be notified to the Data Controller. In the event of any conflict between certain provisions of this DPA and the provisions of Terms of Service, the provisions contained in the DPA shall prevail over such conflicting provisions of the Addendum solely with respect to the Processing of Personal Data. IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Services Agreement with effect from the date first set out above.

Exhibit 1

Standard Contractual Clauses (processors)

Background

The data exporter has entered into a data processing Agreement ("Agreement") with the data importer. Pursuant to the terms of the Agreement, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with modernised SCC issued by the EU Commission on June 4, 2021 and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

2. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
2. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
3. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
4. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
5. Clause 13;
6. Clause 15.1(c), (d) and (e);
7. Clause 16(e);
8. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18. (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Section II – Obligations of the Parties

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This

Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects.

The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

1. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

2. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

3. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

4. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least one month in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this

regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

1. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

2. refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and

comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

1. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

2. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

3. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

2. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

1. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

2. the data importer is in substantial or persistent breach of these Clauses; or

3. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
   In these cases, it shall inform the competent supervisory of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.

The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these

Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the EU Member State in which the data exporter is established.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Data Exporter is the Customer who enters into a Service Agreement with the Data Importer to obtain a SurveySparrow Account as defined in the Terms of Service and has access to use the Services including its Affiliates.

Data importer(s):

The data importer is SurveySparrow Inc. who provides Services to the Data Exporter pursuant to Terms of Service.

Data Protection Officer: CM Balaji, VP of Engineering

B. DESCRIPTION OF TRANSFER

- **Categories of data subjects whose personal data is transferred**

Include the Data Controller's employees, contractors, customers, prospects, suppliers and subcontractors.

- **Categories of personal data transferred**

This includes contact information, the extent of which is determined and controlled by the Customer in its sole discretion, and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by end users via the Services.

- Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The parties do not anticipate the transfer of special categories of data from whom the Survey Responses or Personal Data is collected by the Data Controller.

- The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Transfer takes place only during the duration of the Terms of Service subject to Clause 8 of this Data Protection Addendum.

- Nature of the processing

The subject-matter of Processing of Personal Data by Data Processor is the provision of the Services to the Data Controller that involves the Processing of Personal Data, as specified in the Terms of Service.

- Purpose(s) of the data transfer and further processing

Personal Data will be processed for purposes of providing the Services set out in the Terms of Service.

- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

Personal data will be retained only during the provision of Services pursuant to Terms of Service. Upon termination or expiry of the SurveySparrow account, Upon termination or expiration of the Agreement, Personal Data will not be retained, including any copies thereof except those required for audit and legal purposes.

- For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As applicable to the Data Processor.

C. COMPETENT SUPERVISORY AUTHORITY

DATA PROTECTION COMMISSION

21 FITZWILLIAM SQUARE SOUTH

DUBLIN 2

D02 RD28

IRELAND

ANNEX II – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. Data Protection Officer/Executives

- Each party will designate a person who will be incharge of communication between the parties via email so as to execute any specific instructions. These officers will serve as the primary point of contact at either party's end.

2. Security Practices

- Data Processor takes regular backups of customer data to prevent any major data loss during a security incident.
- All data stored is encrypted so that the customer's personal data is stored securely.
- Servers and data are managed by Amazon Web Services (AWS – Cloud Computing Services).

- Security policies and security groups are intact so that only authorized people have access to Servers.

Please see our security page for more information.

3. Measures of pseudonymisation and encryption of personal data

Encryption

- Data Processor makes HTTPS encryption (encrypts your data in transit using secure TLS Cryptographic Protocols) available on every one of its login interfaces and for free & paid customers, alike.

4. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

a. Access Control

- Processor maintains and updates a record of security privileges of its personnel that have access to Customer Data, networks and network services.
- Processor ensures that, each personnel having access to its systems have a single unique identifier/log-in.
- Processor has user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Data systems and networks, based on the job role.

b. Integrity and Confidentiality

- The site that is used to access resources will be logged out automatically everyday. Only authorized personnel inside the organization can access these e portals.

c. Authentication

- The Data Processor has enabled Multi Factor Authentication as a second layer to ensure that only authorized personnel access the platform.

d. Operations Security

- Processor maintains policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data and to its systems and networks.
- Processor maintains multiple copies of Customer Data from which Customer Data can be recovered in case of a breach.
- Processor maintains logs and monitors access to administrator and operator activity and data recovery events.

5. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Security Incident Management & Business Continuity

- Processor will maintain a record of all security incidents, their respective RCA findings & risk mitigation adopted.
- In case a security incident happens due to unforeseen circumstances, the Processor will inform the Point of Contact of the Controller via Email within 48 hours.
- Risk Mitigation will be carried out to ensure restoration of data from the Data Backup, to support continuity of business.

6. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- Data Processor conducts VAPT on an annual basis.
- Information Security audit is planned and conducted along with the organizational level audit (annual internal audit.

7. Measures for the protection of data during transmission

- All the data transferred from in and out of SurveySparrow is secured with HTTPS.

8. Measures for the protection of data during storage

- SurveySparrow uses Advanced Encryption Standard (AES) algorithm in Galois/Counter Mode (GCM) with 256-bit secret keys to encrypt the data at rest.

9. Measures for ensuring physical security of locations at which personal data are processed

Physical and Environmental Security

- Data centers maintained by AWS are secure by design and its controls make that possible.
- The workplace however, is guarded all the time and people with access can only enter. Please see our security page for more information.

10. Measures for certification/assurance of processes and products

- Data Processor is certified for ISO 27001:2013. This demonstrates the direction and commitment of the Data Processor to information security in order to protect its own information assets and those provided by the Data Controller.

11. Measures for ensuring data quality

- The quality assurance process of the Data Processor, besides performing functional validation and verification, also runs a thorough security check on all application updates. The validation process is carried out by our dedicated app security team who aim to discover and rectify all vulnerabilities in the application.
- Application updates are not approved by Data Processor's quality assurance team unless all liable vulnerabilities are identified.

12. Measures for ensuring limited data retention

- When an account is deleted, all data associated with the account is destroyed within a week. Data Processor also offers data export options which Data Controllers can use if they want a backup of their data before deletion. For more information regarding data deletion, please refer to our Privacy policy.

13. Organization of Information Security

- Processor has appointed a Security Officer responsible for coordinating and monitoring the security rules and procedures.
- The Security Officer is bound by confidentiality obligations.

14. Human Resources Security

- A background check will be conducted on the employee(s) that will have access servers to rule out any criminal involvement.
- Processor will make sure to train its employees that will be handling Controller's Data about their roles and security guidelines that will have to be adhered to from time to time.
- In case of any violation by its employees, Processor will take disciplinary action, that could also include termination of the employee from the Processor's organization.

15. System Acquisition, Development and Maintenance

- Processor has policies for secure development, system engineering and support. Processor conducts appropriate tests for system security as part of acceptance testing processes.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

- The data shall be encrypted during its transmission and while at rest.
- Https communication is ensured.

ANNEX III – LIST OF SUB-PROCESSORS

Name	Service Provided	Purpose	Data Centers
Amazon Web Services	Cloud service provider	Cloud infrastructure provider for SurveySparrow. Almost all data stored, processed and transmitted in SurveySparrow resides on Amazon Web Services data centers.	India (Mumbai), USA (Virgina), Canada (Montreal), EU (Frankfurt), UAE (Dubai) depending on customer preference
Hubspot Inc.	CRM	This is our internal cloud based CRM tool used to keep our	United States

		customer contact details and communications up to date as part of the provision of our services.	
Sparkpost,	Email Service Provider	Sending out emails	United States, European Union
Newrelic	Application and Performance Monitoring	To monitor the performance of the application and tune it.	United States, Europe
Stripe	Payment Solution	Subscription is managed by Stripe	United States
Twilio	Messaging	SMS share utilizes Twilio to deliver messages	United States
Google Translate	Translation	Survey and Response Translation provider for SurveySparrow	United States, Europe
Logz.io	Log Management	Managing the logs created in SurveySparow	United States, Europe
Zendesk	CRM	Internal cloud based customer support tool which is used to keep our customer contact details and	United States

		communications up to date as part of the provision of our services.	
Heap Analytics	Analytics tool	An web based analytics tool used to track App events and measure user action on the product including page views, taps, swipes etc.	United States