END USER TERMS OF USE
(Purchased via a Partner)

END USER SHALL AGREE TO THE FOLLOWING TERMS OF USE ('TERMS OF USE' or 'AGREEMENT') IN ORDER TO ACCESS THE SURVEYMONKEY SERVICES.

Signatures

By signing below, the parties agree to be bound by the terms of this Agreement as of the Effective Date.

	END USER		**SurveyMonkey Inc.**
Signed:		Signed:	
Print name:		Print name:	
Title:		Title:	
Date signed:		Date signed:	

Main Terms

1. *DEFINITIONS.*

"**Affiliate**" means any entity which directly or indirectly controls, is controlled by or is under common control with an entity. "Control" for purposes of the preceding sentence means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Article 28**" means article 28 of the General Data Protection Regulation (Regulation (EU) 2016/679). "**Customer**" or

"**you**" means the End User identified on the Subscription Document..

"**Customer Data**" means all data (including Personal Data and End User data) that is provided to SurveyMonkey by, or on behalf of, Customer through Customer's use of the Services, and any data that third parties submit to Customer through the Services.

"**CCPA"** means the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 - 1798.199).

"**Data Protection Impact Assessment"** means a data protection impact assessment as referred to in article 35 of the General Data Protection Regulation (Regulation (EU) 2016/679).

"**Data Protection Legislation"** means (i) the GDPR and all other applicable EU, EEA or European single market Member State laws or regulations or any update, amendment or replacement of same that apply to processing of personal data under this Agreement; (ii) all U.S. laws and regulations that apply to processing of personal data under these Terms of Use including but not limited to CCPA; (iii) all laws and regulations that apply to processing of personal data under these Terms of Use from time to time in place in the United Kingdom and Canada, and the terms "controller", "data subject", "data protection impact assessment", "personal data", "process", "processing", "processor", "supervisory authority" have the same meanings as in the GDPR and with respect to CCPA (as defined above).

"**End Users**" means Customer's employees, agents, independent contractors, and other individuals authorized by Customer to access and use the Services.

"**Intellectual Property Rights**" means current and future worldwide rights under patent, copyright, design rights, trademark, trade secrets, domain names and other similar rights, whether registered or unregistered.

"**SurveyMonkey**" means the SurveyMonkey entity defined in the Subscription Document (SurveyMonkey Contracting Entity).

"**Personal Data**" means information relating to a living individual who is, or can be, reasonably identified from information, either alone or in conjunction with other information (a **"Data Subject"**), within Customer's control and which is stored, collected or processed within one of Customer's SurveyMonkey End User accounts.

"**Services**" means the products and services offered by SurveyMonkey and accessed by Customer as detailed on the Subscription Document.

"**SSTs**" means service-specific terms that apply to specific Services located at https://www.surveymonkey.com/mp/legal/which-terms-apply/ and that are incorporated into and form a part of this

Agreement.

"**Standard Contractual Clauses**" means the "Standard Contractual Clauses" annexed to the European Commission Decision of: (i) 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant

to GDPR or (ii) until such times as SurveyMonkey has entered into the Standard Contractual Clauses outlined at the 5 February 2010 for the Transfer of Customer Personal Data to Processors established in Third Countries under Directive 95/46/EC and where the UK GDPR applies, the applicable standard data protection clauses for processors adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs") or (iii) such other standard contractual clauses or contract terms as may be amended or approved now or in the future for the purposes of facilitating transfer of personal data across borders.

"Subscription Document" means any document entered into between Customer and Pass Through Partner of SurveyMonkey authorising Customer use of Services for a specified term.

2. *SERVICES.*

2.1. Provision of Services. SurveyMonkey will provide the Services to Customer in accordance with this Agreement, as further specified in the Subscription Document and in accordance with any applicable SSTs.

2.2. RESERVED.

2.3. Third-Party Services. If Customer integrates the Services with any non-SurveyMonkey-provided third-party service (such as a third party's service that uses an application programming interface (API)), Customer acknowledges that such thirdparty service might access or use Customer Data and Customer permits the third-party service provider to access Customer Data as required for the interoperation of that third-party service with the Services. Customer is solely responsible for the use of such third-party services and any data loss or other losses it may suffer as a result of using any such services.

3. *SaaS SERVICES.*

3.1. License and Term.

(a) License. Where access to Services are provided as a subscription via the Subscription Document SurveyMonkey grants Customer a non-exclusive, non-transferable worldwide right to access and use the Services during the subscription term, subject to the terms of this Agreement.

(b) Subscription Term. The initial term of each subscription is specified on the Subscription Document.

4. *SERVICE FEATURES.*

4.1. Changes to Services. SurveyMonkey continually changes and improves the Services. SurveyMonkey will provide Customer with prior written notice if SurveyMonkey makes a change to the Service(s) resulting in a material decrease in core functionality used by SurveyMonkey's general customer base. In such event, the parties agree to work together to minimize the impact of such change to Customer.

5. *RESERVED.*

6. CUSTOMER OBLIGATIONS.

6.1. Customer Responsibilities.

(a) Account Security. Customer is responsible for maintaining the confidentiality of its own passwords and any other credentials used by it and its End Users to access the Services. Customer will use commercially reasonable efforts to prevent unauthorized use of the Services and will terminate any unauthorized use of which it becomes aware. Customer will notify SurveyMonkey promptly if Customer becomes aware of any unauthorized access to its accounts.

(b) End User Activities. Customer is responsible for ensuring that its End Users comply with this Agreement. Customer is responsible for the acts of its End Users and any activity occurring in its End User accounts (other than activity that SurveyMonkey is directly responsible for which is not performed in accordance with Customer's instructions).

(c) One Individual per Account. End User accounts and passwords may not be shared and may only be used by one individual per account.

6.2. Acceptable Uses by Customer. Customer agrees to comply with the Acceptable Uses Policy located at https://www.surveymonkey.com/mp/legal/acceptable-uses-policy/.

6.3. Third-Party Requests. The parties may from time to time receive a request from a third-party for records related to Customer's use of

the Services, including information in a Customer End User account or identifying information about a Customer End User, excluding Data Subject access requests as provided for under the GDPR ("**Third-Party Request**"). Third-Party Requests include search warrants, subpoenas, and other forms of legal process.

Customer is responsible for responding to Third Party Requests via its own access to the information and will only contact SurveyMonkey if Customer is unable to obtain such information after diligent efforts. If SurveyMonkey receives a valid Third-Party Request then, to the extent permitted by law, SurveyMonkey:

(a) may inform the third-party issuing such request that it should pursue the request directly with Customer; and

(b) will: (i) promptly notify Customer of the Third-Party Request; (ii) cooperate, at Customer's expense, with Customer's reasonable requests regarding Customer's efforts to oppose a Third Party Request; and (iii) after providing Customer with an opportunity to respond to or oppose the Third-Party Request, SurveyMonkey may fulfil that request if SurveyMonkey determines that it is required or permitted by law to do so.

6.4. Embargoes. Customer represents and warrants that it is not barred by any applicable laws from being supplied with the Services. The Services may not be used in any country that is subject to an embargo by the United States or European Union applicable to the Services. Customer will ensure that: (a) its End Users do not use the Services in violation of any export restriction or embargo by the United States; and (b) it does not provide access to the Services to persons on the U.S. Department of Commerce's Denied Persons List or Entity List, or the U.S. Treasury Department's list of Specially Designated Nationals.

6.5. Suspension of Services. SurveyMonkey may limit or suspend the Services to perform scheduled maintenance or to stop a violation of Section 6.2 (Acceptable Uses by Customer), to prevent material harm to SurveyMonkey or its customers or as required by applicable law. SurveyMonkey will use reasonable endeavours to give Customer reasonable advance notice of any limitation or suspension so that Customer can plan around it or address the issue that has prompted SurveyMonkey to take such action. There may be some situations, such as security emergencies, where it is not practicable for SurveyMonkey to give such advance notice. SurveyMonkey will use commercially reasonable efforts to narrow the scope and duration of the limitation or suspension as is needed to resolve the issue that prompted such action.

7. *SECURITY AND PRIVACY.*

7.1. Security. SurveyMonkey has, considering the state of the art, cost of implementation, the nature, scope, context and purposes of the Services, and the level of risk, implemented appropriate technical and organizational measures to enable a level of security appropriate to the risk of unauthorized or unlawful processing, accidental loss of and/or damage to Customer Data. At reasonable intervals, SurveyMonkey tests and evaluates the effectiveness of these technical and organizational measures for enabling the security of the processing. SurveyMonkey shall ensure security measures equal to or greater than those contained at Appendix 2 (Technical and Organizational Security Measures) are maintained during the term of these Terms of Use.

7.2. Data Protection. Where SurveyMonkey is processing Personal Data for Customer, SurveyMonkey will:

(a) only do so on documented Customer instructions and in accordance with applicable law, including with regard to transfers of Personal Data to other jurisdictions or an international organization, and the parties agree that these Terms of Use constitute such documented instructions of the Customer to SurveyMonkey to process Customer Data;

(b) to the extent applicable, for data transfers SurveyMonkey Europe UC relies upon the Standard Contractual Clauses and/or consent for personal data transfers to countries that do not have adequate levels of data protection as determined by the European Commission, United Kingdom or other jurisdictions which approve and require Standard Contractual Clauses;

(c) with respect to any transfers of Personal Data out of the European Economic Area (EEA), the United Kingdom or other country requiring Standard Contractual Clauses, that may be required in relation to or in connection with the Terms of Use and the provision of the Services hereunder, the parties shall comply with and be subject to all obligations imposed on a 'data importer' or 'data exporter' (as appropriate) as set out under the Standard Contractual Clauses;

(d) ensure that all SurveyMonkey personnel involved in the processing of Personal Data are subject to confidentiality obligations in respect of the Personal Data;

(e) make available information necessary for Customer to demonstrate compliance with its Article 28 obligations (if applicable to the Customer) where such information is held by SurveyMonkey and is not otherwise available to Customer through its account and user areas or on SurveyMonkey websites, provided that Customer provides SurveyMonkey with at least 14 days' written notice of such an information request;

(f) cooperate as reasonably requested by Customer to enable Customer to comply with any exercise of rights by a Data Subject afforded to Data Subjects by Data Protection Legislation in respect of Personal Data processed by SurveyMonkey in providing the Services; provide assistance, where necessary with all requests received directly from a Data Subject in respect of a Data Subject's Personal Data submitted through the Services;

(g) upon deletion, by you, not retain Customer Personal Data from within your account other than in order to comply with applicable laws and regulations and as may otherwise be kept in routine backup copies made for disaster recovery and business continuity purposes subject to our retention policies;

(h) cooperate with any supervisory authority or any replacement or successor body from time to time (or, to the extent

required by the Customer, any other data protection or privacy regulator under Data Protection Legislation) in the performance of such supervisory authority's tasks where required;

(i) not store Personal Data (in a format that permits identification of relevant Data Subjects) for longer than is necessary for the purposes for which the data is processed save to the extent such retention is required for legitimate business purposes (with respect to, for example, security and billing), in order to comply with applicable laws and regulations and as may otherwise be kept in routine backup copies made for disaster recovery and business continuity purposes;

(j) where required by Data Protection Legislation, inform Customer if it comes to SurveyMonkey's attention that any instructions received from Customer infringe the provisions of Data Protection Legislation, provided that notwithstanding the foregoing, SurveyMonkey shall have no obligation to review the lawfulness of any instruction received from the Customer. If this provision is invoked, SurveyMonkey will not be liable to Customer under the Terms of Use for any failure to perform the applicable Services until such time as Customer issues new lawful Instructions with regard to the Processing; and

(k) assist Customer as reasonably required where Customer (i) conducts a data protection impact assessment involving the Services (which may include by provision of documentation to allow customer to conduct their own assessment); or (ii) is required to notify a Security Incident (as defined below) to a supervisory authority or a relevant data subject.

7.3. Use of Sub-processors. Customer provides a general authorization to SurveyMonkey to engage onward sub- processors, subject to compliance with the requirements in this Section 7. SurveyMonkey will, subject to any confidentiality provisions under this Terms of Use or otherwise imposed by SurveyMonkey:

(a) make available to Customer a list of the SurveyMonkey subprocessors ("**Sub-processors**") who are involved in processing or sub-processing Personal Data in connection with the provision of the Services, together with a description of the nature of services provided by each Sub-processor ("**Sub-processor List**"). A copy of this Sub-processor List may be accessed at http://www.surveymonkey.com/mp/legal/subprocessorlist/?ut_source=legal&ut_source2=general&ut_source3=inline;

(b) ensure that all Sub-processors on the Sub-processor List are bound by contractual terms that are in all material respects no less onerous than those contained in this Agreement; and

(c) be liable for the acts and omissions of its Sub-processors to the same extent SurveyMonkey would be liable if performing the services of each of those Sub-processors directly under the terms of this Agreement.

7.4. New / Replacement Sub-processors. SurveyMonkey will provide Customer with written notice of the addition of any new Sub-processor or replacement of an existing Sub-processor at any time during the term of the Terms of Use("**New Subprocessor Notice**"). Customer will sign up to a mailing list at https://surveymonkey.knack.com/subprocessorlist?ut_source=legal&ut_source2=subprocessor-list&ut_source3=inline#subprocessorlist/addsubscriber/ made available by SurveyMonkey through which such notices will be delivered by e-mail or alternatively will check on updates to the list at https://www.surveymonkey.com/mp/legal/subprocessor-list/?ut_source=legal&ut_source2=general&ut_source3=inline. If Customer has a reasonable basis related to data protection to object to SurveyMonkey's use of a new or replacement Subprocessor, Customer will notify SurveyMonkey promptly in writing and in any event within 30 days after receipt of a New Sub-processor Notice. In the event of such reasonable objection, either Customer or SurveyMonkey may terminate the portion of any Terms of Use relating to the Services that cannot be reasonably provided without the objected-to new Subprocessor (which may involve termination of the entire Agreement) with immediate effect by providing written notice to the other party.

7.5. Audits. Customer will provide SurveyMonkey with at least one month's prior written notice of any audit, which may be conducted by Customer, or an independent auditor appointed by Customer (provided that no person conducting the audit shall be, or shall act on behalf of, a competitor of SurveyMonkey) ("**Auditor**"). The scope of an audit will be as follows:

(a) Customer will only be entitled to conduct an audit once per year unless otherwise legally compelled or required by a regulator with established authority over the Customer to perform or facilitate the performance of more than 1 audit in that same year (in which circumstances Customer and SurveyMonkey will, in advance of any such audits, agree upon a reasonable reimbursement rate for SurveyMonkey's audit expenses).

(b) SurveyMonkey agrees, subject to any appropriate and reasonable confidentiality restrictions, to provide evidence of any certifications and compliance standards it maintains and will, on request, make available to Customer an executive summary of SurveyMonkey's most recent annual penetration tests, which summary shall include remedial actions taken by SurveyMonkey resulting from such penetration tests.The scope of an audit will be limited to SurveyMonkey systems, processes, and documentation relevant to the processing and protection of Personal Data, and Auditors will conduct audits subject to any appropriate and reasonable confidentiality restrictions requested by SurveyMonkey.

(c) Customer will promptly notify and provide SurveyMonkey with full details regarding any perceived non- compliance or security concerns discovered during the course of an audit.

The parties agree that, except as otherwise required by order or other binding decree of a regulator with authority over the Customer, this Section 7.6 sets out the entire scope of the Customer's audit rights as against SurveyMonkey.

7.6. Security Incident. If SurveyMonkey becomes aware of any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Personal Data ("**Security Incident**"), SurveyMonkey will notify Customer without undue delay.

Such notification shall not be interpreted or construed as an admission of fault or liability by SurveyMonkey. A Security Incident does not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems. SurveyMonkey will also reasonably cooperate with Customer with respect to any investigations relating to a Security Incident with preparing any required notices, and provide any information reasonably requested by Customer in relation to any Security Incident.

7.7. Customer Privacy Obligations. Customer shall ensure and hereby warrants and represents that it is entitled to transfer the Customer Data to SurveyMonkey so that SurveyMonkey may on behalf of Customer, lawfully process and transfer the Personal Data in accordance with this Agreement. Customer shall ensure that relevant Data Subjects have been informed of, and have given their consent to, such use, processing, and transfer as required by all applicable data protection legislation.

7.8. Types of Data Processing. The parties agree that the purpose and nature of the processing of Personal Data, the types of Personal Data and categories of Data Subjects are as set out in Appendix 1.

8. *INTELLECTUAL PROPERTY.*

8.1. Customer IP. As between the parties, the Customer retains ownership of all Intellectual Property Rights in the Customer Data. These Terms of Use do not grant SurveyMonkey any licenses or rights to the Customer Data except for the following:

(a) Customer grants SurveyMonkey and its affiliates a worldwide, royalty-free, non-exclusive, limited license to use, host, copy, transmit, modify, display, and distribute Customer Data only for the limited purposes of providing the Services to Customer and improving the Services subject to the use of privacy minimization techniques such as de-identification and pseudonymization where possible and appropriate.

(b) If Customer provides SurveyMonkey with feedback about the Services, SurveyMonkey may use that feedback and incorporate it into its products and services without any obligation to Customer.

8.2. SurveyMonkey IP. As between the parties, SurveyMonkey retains ownership of the Services and all related Intellectual Property Rights. No licenses or rights are granted to Customer by SurveyMonkey other than as expressly provided for in this Agreement. These Terms of Use do not grant the Customer any right to use SurveyMonkey's trademarks or other brand elements except as may be otherwise agreed in writing between the parties.

8.3. Publicity. SurveyMonkey may identify Customer by name and logo as a SurveyMonkey customer on SurveyMonkey's website and on other promotional materials. Any goodwill arising from the use of Customer's name and logo will inure to the benefit of Customer.

9. *CONFIDENTIALITY.*

9.1. Definition. "**Confidential Information**" means information disclosed by a party ("**Discloser**") to the other party ("**Recipient**") in connection with the use or provision of the Services that is either marked as confidential or would reasonably be considered as confidential under the circumstances. Customer's Confidential Information includes Customer Data. SurveyMonkey's Confidential Information includes the terms of these Terms of Use and any security information about the Services. Despite the foregoing, Confidential Information does not include information that: (a) is or becomes public through no fault of the Recipient; (b) the Recipient already lawfully knew; (c) was rightfully given to the Recipient by an unaffiliated third party without restriction on disclosure; or (d) was independently developed by the Recipient without reference to the Discloser's Confidential Information.

9.2. Confidentiality. The Recipient will: (a) protect the Discloser's Confidential Information using commercially reasonable efforts; (b) use the Discloser's Confidential Information only as permitted by this Agreement, including to exercise the Recipient's rights and fulfil the Recipient's obligations under this Agreement; and (c) not disclose the Discloser's Confidential Information without the Discloser's prior consent, except to affiliates, contractors, agents, and professional advisors who need to know it and have agreed in writing (or, in the case of professional advisors, are otherwise bound) to keep it confidential on terms comparable to those under this Section. The Recipient may disclose the Discloser's Confidential Information when and to the extent required by law or legal process, but only after the Recipient, if permitted by law, uses reasonable efforts to notify the other party.

9.3 Return or Destruction of Confidential Information. Upon the termination or expiration of the Terms of Use and any associated Subscription Documents hereunder, each party will promptly return to the other party or destroy all Confidential Information of the other party in its possession or control within a reasonable amount of time in accordance with the Recipient's data destruction practices. Despite the termination or expiration of this Agreement, Recipient's confidentiality obligations with respect to the Confidential Information will survive for two (2) years after the date such Confidential Information was disclosed to Recipient (except with respect to any trade secrets identified by Discloser as such at the time of disclosure, where such confidentiality obligations will continue for as long as the information remains a trade secret).

10. *WARRANTIES.*

10.1. Warranties. Each party represents and warrants that: (a) it has full power and authority to enter into this Agreement; and (b) it will comply with all laws and regulations applicable to its provision or use of the Services. SurveyMonkey further represents and warrants that the Services shall conform to, and perform in accordance with, any applicable specifications, and shall otherwise be free from any material defects. SurveyMonkey shall provide the Services in a good and workmanlike manner, in accordance with industry standards, and with that standard of care, skill, and diligence normally provided by similar professionals in the performance of similar services.

10.2. Disclaimers. SURVEYMONKEY MAKES NO REPRESENTATION OR WARRANTY ABOUT THE SERVICES. TO THE FULLEST EXTENT PERMITTED UNDER APPLICABLE LAW, SURVEYMONKEY DISCLAIMS ANY IMPLIED OR STATUTORY WARRANTY, INCLUDING ANY WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

11. *INDEMNIFICATION.*

11.1. By SurveyMonkey. If a third party claims that the Services SurveyMonkey provides to you infringe or misappropriate that party's Intellectual Property Rights, SurveyMonkey will defend you against that claim at its expense and pay all costs, damages and attorney's fees that a court finally awards or that are included in a settlement approved by SurveyMonkey. However, in no event will SurveyMonkey have any obligation or liability arising from: (a) use of any Services in a modified form or in combination with software, technologies, products, or devices not provided by SurveyMonkey or intended as part of the use

of the Services; or (b) any content or data provided by Customer, End Users, or third parties; or (c) Services for which there is no fee or charge.

11.2. By Customer. If a third party claims that the Customer Data infringes or misappropriates that third party's Intellectual Property Rights or if Customer's use of the Services violates the SurveyMonkey Acceptable Use Policy, Customer will defend SurveyMonkey against any such claim or investigation at Customer's expense and pay all costs, damages and attorney's fees that a court finally awards or that are included in a settlement approved by Customer.

11.3. Potential Infringement. If SurveyMonkey believes the technology used to provide the Services may infringe or may be alleged to infringe a third party's Intellectual Property Rights, then SurveyMonkey may: (a) obtain the right for Customer, at SurveyMonkey's expense, to continue using the Services; (b) provide a non-infringing functionally equivalent replacement; or (c) modify the Services so that they no longer infringe. If SurveyMonkey does not believe that the foregoing options are commercially reasonable, then SurveyMonkey may suspend or terminate Customer's use of the impacted Services and provide a pro rata refund of any fees prepaid by Customer applicable to the period following the termination of such Services.

11.4. Indemnity Procedures. A party seeking indemnification will promptly notify the other party of the claim and reasonably cooperate with the other party (to the extent applicable) in defending the claim. The indemnifying party will have full control and authority over the defense, except that: (a) any settlement requiring the indemnified party to admit liability, perform any act or to pay any money will require that indemnified party's prior written consent (such consent not to be unreasonably withheld or delayed) and (b) the indemnified party may join in the defense with its own counsel at its own expense. The provisions of this Section 11 state each party's entire liability and constitute the other party's sole and exclusive financial remedy for any indemnification claims. Notwithstanding the foregoing, nothing in these Terms of Use will prevent either party from seeking injunctive relief with respect to a violation of intellectual property rights, confidentiality obligations or enforcement or recognition of any award or order in any appropriate jurisdiction.

12. *LIABILITY.*

12.1. Consequential Damages Waiver. TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY BE LIABLE UNDER OR IN CONNECTION WITH THESE TERMS OF USEFOR: (A) ANY INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE OR EXEMPLARY DAMAGES, UNDER ANY THEORY OF LAW, INCLUDING TORT OR (B) LOSS OF OR DAMAGE TO: (i) DATA, (ii) BUSINESS, (iii) REVENUES, OR (iv) PROFITS (IN EACH CASE WHETHER DIRECT OR INDIRECT), EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE, AND EVEN IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

12.2. Liability Cap. TO THE EXTENT PERMITTED BY APPLICABLE LAW, AND NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, EACH PARTY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR IN CONNECTION WITH THESE TERMS OF USE FOR ALL CLAIMS OF ANY KIND WILL NOT EXCEED THE AMOUNTS PAID OR PAYABLE BY CUSTOMER TO SURVEYMONKEY UNDER THESE TERMS OF USE DURING THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO THE LIABILITY ("GENERAL CAP"). NOTWITHSTANDING THE FOREGOING, EACH PARTY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR IN CONNECTION WITH THE TERMS OF USE FOR ALL CLAIMS RELATED TO A PARTY'S BREACH OF ITS OBLIGATIONS UNDER SECTION 7 ("SECURITY AND PRIVACY") AND SECTION 9 ("CONFIDENTIALITY") ABOVE SHALL NOT EXCEED TWO (2) TIMES THE AMOUNT OF FEES ACTUALLY PAID BY THE CUSTOMER UNDER THE TERMS OF USE DURING THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO THE LIABILITY ("ENHANCED CAP").

12.3. Excluded Claims. SECTIONS 12.1 AND 12.2 SHALL NOT APPLY TO CLAIMS RELATED TO: (A) A PARTY'S INDEMNIFICATION OBLIGATIONS, (B) FRAUD OR WILFUL MISCONDUCT, (C) DEATH OR PERSONAL INJURY, OR (D) CUSTOMER'S OBLIGATION TO PAY ANY UNDISPUTED FEES OR INVOICES.

13. *TERM AND TERMINATION.*

13.1. Term of Terms of Use The term of these Terms of Use start on the Effective Date of the Subscription Document and shall remain in effect until end of the Subscription Term contained therein.

13.2. Termination for Cause. A party may terminate these Terms of Use (including all related Order Forms): (a) upon 30 days' written notice to the other party of a material breach if such breach remains uncured at the expiration of such period; or (b) if the other party ceases its business operations or becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency,

receivership, administration, liquidation, or assignment for the benefit of creditors.

13.3. Consequences of Termination of Agreement. If these Terms of Use terminates, any Subscription Documents in effect will remain in effect in accordance with their terms (including the terms of these Terms of Use that are incorporated by reference)..

13.4. Survival. The following Sections will survive any expiration or termination of the Terms of Use: 5 and 9 to 15.

14. *RESERVED*

15. GENERAL.

15.1. Force Majeure. Neither SurveyMonkey nor Customer will be liable for any delay, inadequate performance or failure to perform any obligations under these Terms of Use to the extent caused by a condition (including, but not limited to,

natural disaster, act of war or terrorism, earthquake, pandemic or health crisis, riot, governmental order, action or inaction, denial of service attack or utility or internet service provider failure, delay or disturbance) that was beyond the party's reasonable control.

15.2. No Waiver. A party's failure or delay to enforce a provision under these Terms of Use is not a waiver of its right to do so later.

15.3. Notices.

(a) Providing Notice. All notices must be in writing and will be deemed given when: (i) personally delivered, (ii) verified by written receipt, if sent by postal mail with verification of receipt service or courier, (iii) received, if sent by postal mail without verification of receipt, or (iv) verified by automated receipt or electronic logs if sent by email.

(b) Notices to SurveyMonkey. Notices to SurveyMonkey must be sent to SurveyMonkey, One Curiosity Way, San Mateo, CA 94403, USA, marked to the attention of the Legal Department, with a copy to legalnotices@SurveyMonkey.com. Email is insufficient for providing non-routine legal notices (including indemnification claims, breach notices, and termination notices) ("**Non-Routine Legal Notices**") to SurveyMonkey. Customer may grant approvals, permission, extensions, and consents by email.

(c) Notices to Customer. Notices to Customer may be sent to the email address associated with Customer's designated primary administrator for the relevant Service ("**Primary Admin**"). Billing-related notices (including notices of overdue payments) may be sent to the relevant billing contact designated by Customer. If Customer has provided contact details for legal notices on the cover page of this Agreement, any Non-Routine Legal Notices will be provided to such contact instead, with a copy to the email address associated with Customer's Primary Admin.

(d) Keep Contact Details Current. Customer and its End Users must keep the contact details associated with their user accounts and billing contacts current and accurate and notify SurveyMonkey in writing of any changes to such details.

15.4. Precedence. If any conflict exists among the following documents, the order of precedence will be: (1) the applicable Subscription Document, (2) these Terms of Use and (3) the applicable SSTs. Any terms set forth under a "Special Terms" heading in any of the foregoing documents will take precedence over any other terms to the contrary in that document.

15.5. Severability. If any provision of these Terms of Use t is determined to be unenforceable by a court of competent jurisdiction, that provision will be severed, and the remainder of terms will remain in full effect.

15.6. Third-Party Beneficiaries. There are no third-party beneficiaries to these Terms of Use. Customer's End Users are not third-party beneficiaries to Customer's rights hereunder.

15.7. Language. These Terms of Use were prepared and written in English. Any non-English translations which may be made available are provided for convenience only and are not valid or legally binding.

16. *GOVERNMENT TERMS.*

16.1. U.S. Government Terms.

(a) Federal Government Agencies. If Customer is a United States Federal Government Agency, the Amendment located at https://www.surveymonkey.com/mp/legal/terms-of-use-federal-government/ applies to Customer, except that references to the "Agreement" in that Amendment are to be read as references to the Terms of Use , and references to "Content" will refer to Customer Data.

(b) Other U.S. Governmental Entities. If Customer is a different type of governmental entity in the United States, the Amendment located at https://www.surveymonkey.com/mp/legal/terms-of-use-state-government/ applies to Customer, except that references to the "TOU" and "Terms" in that Amendment are to be read as references to these Terms of Use.

17. *CALIFORNIA CONSUMER PRIVACY ACT.*

17.1. CCPA. Where SurveyMonkey is processing "Personal Information" for Customer as defined under the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 - 1798.199) ("CCPA") and in connection with California consumers, the parties hereby agree that SurveyMonkey is a "Service Provider" and Customer is the "Business". As your Service Provider, SurveyMonkey will:

(a) collect, retain, use, disclose and otherwise process Personal Information solely (1) to fulfil its obligations to Customer under this Agreement, on the Customer's behalf, (2) for the Customer's operational purposes, (3) for SurveyMonkey's internal use as permitted by Data Protection Legislation, (4) to detect data security incidents or protect against fraudulent or illegal activity, (5) as otherwise permitted under Data Protection Legislation and (6) for other notified purposes and for no other operational purposes;

(b) cooperate as reasonably requested by Customer (at Customer's expense) to enable Customer to comply with obligations under the CCPA to respond to verifiable consumer requests to delete or access Personal Information processed by SurveyMonkey in providing the Services;

(c) not sell Personal Information or otherwise disclose Personal Information for a commercial purpose; and

(d) hereby certify that it understands the restrictions and obligations set forth in Cal. Civ. Code § 1798.140(w)(2) and will comply with them.

* * * * *

Appendix 1

Purposes and Nature of Personal Data Processing, Categories of Personal Data, Data Subjects

Purposes and Nature of Processing	SurveyMonkey may Process Personal Data as necessary to technically perform the Services, including where applicable: • Hosting and storage; • Backup and disaster recovery; • Technically improve the service; • Service change management; • Issue resolution; • Providing secure, encrypted Services; • Applying new product or system versions, patches, updates and upgrades; • Monitoring and testing system use and performance; • Proactively detect and remove bugs; • IT security purposes including incident management; • Maintenance and performance of technical support systems and IT infrastructure; • Migration, implementation, configuration and performance testing; • Making product recommendations; • Providing customer support; transferring data, and • Assisting with Data Subject requests (as necessary).
Categories of Personal Data	The Customer may submit personal data to the Services, and may request for the Customer's respondents to submit personal data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, without limitation: Personal data of all types that may be submitted by the Customer's respondents to the Customer via user of the Services (such as via surveys or other feedback tools). For example: name, geographic location, age, contact details, IP address, profession, gender, financial status, personal preferences, personal shopping or consumer habits, and other preferences and other personal details that the Customer solicits or desires to collect from its respondents. Personal data of all types that may be included in forms and surveys hosted on the Services for the Customer (such as may be included in survey questions). The Customer's respondents may submit special categories of personal data to the Customer via the Services, the extent of which is determined and controlled by the Customer. For clarity, these special categories of Personal Data may include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade- union membership, and the processing of data concerning health or sex life.

Data Subjects	Data subjects include: Natural persons who submit personal data to SurveyMonkey via use of the Services (including via online surveys and forms hosted by SurveyMonkey on behalf of the Customer); Natural persons whose personal data may be submitted to the Customer by Respondents via use of the Services; Natural persons who are employees, representatives, or other business contacts of the Customer; The Customer's users who are authorized by the Customer to access and use the Services.

Appendix 2

Technical and Organizational Security Measures

SurveyMonkey will maintain appropriate administrative, physical, and technical safeguards ("**Security Safeguards**") for protection of the security, confidentiality and integrity of personal data provided to it for provision of the Services to the Customer.

The Security Safeguards include the following:

(a) Domain: Organization of Information Security.

(i) **Security Roles and Responsibilities.** SurveyMonkey personnel with access to data are subject to confidentiality obligations.

(ii) **Risk Management Program.** SurveyMonkey performs a risk assessment where appropriate before processing the data.

(b) Domain: Asset Management.

(i) *Asset Handling.*

(1) SurveyMonkey has procedures for disposing of printed materials that contain Customer Data.

(2) SurveyMonkey maintains an inventory of all hardware on which Customer Data is stored.

(c) Domain: Human Resources Security.

(i) *Security Training.*

(1) SurveyMonkey informs its personnel about relevant security procedures and their respective roles. SurveyMonkey also informs its personnel of possible consequences of breaching the security rules and procedures.

(d) Domain: Physical and Environmental Security.

(i) **Physical Access to Facilities.** SurveyMonkey limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.

(ii) **Protection from Disruptions.** SurveyMonkey uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

(iii) **Component Disposal.** SurveyMonkey uses industry standard processes to delete Customer Data when it is no longer needed.

(e) Domain: Communications and Operations Management.

(i) **Operational Policy.** SurveyMonkey maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.

(f) Data Recovery Procedures.

(1) On a regular and ongoing basis, SurveyMonkey creates backup copies of Customer Data from which Customer Data may be recovered in the event of loss of the primary copy.

(2) SurveyMonkey stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

(3) SurveyMonkey has specific procedures in place governing access to copies of Customer Data.

(ii) Malicious Software. SurveyMonkey has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks.

(g) Data Beyond Boundaries.

(1) SurveyMonkey encrypts Customer Data that is transmitted over public networks.

(h) Event Logging.

(1) SurveyMonkey logs the use of its data-processing systems.

(2) SurveyMonkey logs access and use of information systems containing Customer Data, registering the access ID, timestamp, and certain relevant activity.

(i) Domain: Information Security Incident Management.

(i) *Incident Response Process.*

(1) SurveyMonkey maintains an incident response plan.

(2) SurveyMonkey maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and remediation steps, if applicable.

(j) Domain: Business Continuity Management.

(i) SurveyMonkey's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original state from before the time it was lost or destroyed.

(k) Access Control to Processing Areas.

Processes to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the Customer Personal Data are processed or used, to include:

(i) establishing secure areas;

(ii) protection and restriction of access paths;

(iii) securing the mobile/cellular telephones;

(iv) data processing equipment and personal computers;

(v) all access to the data centres where Customer Personal Data are hosted is logged, monitored, and tracked;

(vi) the data centres where Customer Personal Data are hosted is secured by a security alarm system, and other appropriate security measures; and

(vii) the facility is designed to withstand adverse weather and other reasonably predictable natural conditions, is secured by around-the-clock guards, keycard and/or biometric access (as appropriate to level of risk) screening and escort-controlled access, and is also supported by on-site back-up generators in the event of a power failure.

(l) Access Control to Data Processing Systems.

Processes to prevent data processing systems from being used by unauthorized persons, to include:

(i) identification of the terminal and/or the terminal user to the data processor systems;

(ii) automatic time-out after 30 minutes or less of user terminal if left idle, identification and password required to reopen;

(iii) issuing and safeguarding of identification codes;

(iv) password complexity requirements (minimum length, expiry of passwords, etc.); and

(v) protection against external access by means of an industrial standard firewall.

(m) Access Control to Use Specific Areas of Data Processing Systems.

Measures to ensure that persons entitled to use data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Customer Personal Data cannot be read, copied, modified or removed without authorization, to include by:

(i) implementing binding employee policies and providing training in respect of each employee's access rights to the Customer Personal Data; effective and measured disciplinary action against individuals who access Customer Personal Data without authorization;

(ii) release of data to only authorized persons;

(iii) implementing principles of least privileged access to information which contains Customer Personal Data strictly on the basis of "need to know" requirements;

(iv) production network and data access management governed by VPN, two factor authentication, and role-based access controls; application and infrastructure systems log information to centrally managed log facility for troubleshooting, security reviews, and analysis; and

(v) policies controlling the retention of backup copies which are in accordance with applicable laws and which are appropriate to the nature of the data in question and corresponding risk.

(n) Transmission Control.

Procedures to prevent Customer Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Customer Personal Data by means of data transmission facilities is envisaged, to include:

(i) use of firewall and encryption technologies to protect the gateways and pipelines through which the data travels;

(ii) implementation of VPN connections to safeguard the connection to the internal corporate network;

(iii) constant monitoring of infrastructure (e.g. ICMP-Ping at network level, disk space examination at system level, successful delivery of specified test pages at application level); and

(iv) monitoring of the completeness and correctness of the transfer of data (end-to-end check).

(o) Storage Control.

When storing any Customer Personal Data: it will be backed up as part of a designated backup and recovery processes in encrypted form, using a commercially supported encryption solution and all data defined as Customer Personal Data stored on any portable or laptop computing device or any portable storage medium is likewise encrypted. Encryption solutions will be deployed with no less than a 128-bit key for symmetric encryption and a 1024 (or larger) bit key length for asymmetric encryption;

(p) Input Control.

Measures to ensure that it is possible to check and establish whether and by whom Customer Personal Data has been input into data processing systems or removed, to include:

(i) authentication of the authorized personnel;

(ii) protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data; (iii) utilization of user codes (passwords);

(iv) proof established within data importer's organization of the input authorization; and

(v) ensuring that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are locked.

(q) Availability Control.

Measures to ensure that Customer Personal Data are protected from accidental destruction or loss, to include infrastructure redundancy and regular backups performed on database servers.

(r) Segregation of Processing.

Procedures to ensure that data collected for different purposes can be processed separately, to include:

(i) separating data through application security for the appropriate users; storing data, at the database level, in different tables, separated by the module or function they support;

(ii) designing interfaces, batch processes and reports for only specific purposes and functions, so data collected for specific purposes is processed separately; and

(iii) barring live data from being used for testing purposes as only dummy data generated for testing purposes may be used for such.

(s) Vulnerability management program.

A program to ensure systems are regularly checked for vulnerabilities and any detected are immediately remedied, to include:

(i) all networks, including test and production environments, regularly scanned; and

(ii) penetration tests are conducted regularly and vulnerabilities are remedied promptly.

(t) Data Destruction.

In the event of expiration or termination of the Agreement by either side or otherwise on request from the Customer following receipt of a request from a data subject or regulatory body:

(i) all Customer data shall be securely destroyed within 3 months; and

(ii) all Customer data shall be purged from all SurveyMonkey and/or third party storage devices including backups within 6 months of termination or receipt of a request from Customer unless SurveyMonkey is otherwise required by law to retain a category of data for longer periods. SurveyMonkey will ensure that all such data which is no longer required is destroyed to a level where it can be assured that it is no longer recoverable.

(u) Standards and Certifications.

Data storage solutions and/or locations have at least SOC 1 (SSAE 16) or SOC 2 reports – equivalent or similar certifications or security levels will be examined on a case by case basis.