

# SurveyMonkey Data Processing Agreement

## HOW THIS DPA APPLIES

This SurveyMonkey Data Processing Agreement (“DPA”) forms part of your Agreement with SurveyMonkey and contains certain terms relating to data protection, privacy, and security in accordance with the Data Protection Legislation, where applicable. In the event (and to the extent only) that there is a conflict between the different Data Protection Legislation laws and regulations, the parties shall comply with the more onerous requirements or higher standard which shall, in the event of a dispute in that regard, be determined solely by SurveyMonkey.

This DPA is between the Customer and the applicable SurveyMonkey entity determined as follows:

- (i) for Customers located in any country other than the United States, SurveyMonkey Europe UC shall be the contracting entity;
- (ii) for Customers located inside the United States, SurveyMonkey Inc. shall be the contracting entity.

This is the latest version of the DPA (dated April 15, 2025).

## DATA PROCESSING TERMS

### 1. Interpretation

In this DPA the following expressions shall, unless the context otherwise requires, have the following meanings:

- “Agreement” means any agreement between SurveyMonkey Inc. or SurveyMonkey Europe and a customer for the Services. Such an agreement may have various titles, such as “Order Form”, “Sales Order”, “Terms of Use” or “Master or Governing Services Agreement”.
- “Article 28” means article 28 of GDPR and the UK GDPR as applicable to the processing of Customer Personal Data.
- “Customer” or “you” means the customer that is identified on, and/or is a party to, the Agreement.

- “Customer Data” means all data (including but not limited to Customer Personal 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.
- “Customer Personal Data” means all Personal Data that is submitted to the Services by or to Customer, processed by SurveyMonkey for the purposes of delivering the Services to the Customer including but not limited to the personal data set out in Appendix 2 to this DPA.
- “Data Protection Legislation” means all mandatory data protection or privacy laws directly applicable to SurveyMonkey in its capacity as processor or service provider (as the case may be) in relation to the processing of Personal Data under the Agreement, including:
  - (i) the General Data Protection Regulation (Regulation (EU) 2016/679)(“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 applies to processing of personal data under the Agreement;
  - (ii) the Swiss new Federal Act on Data Protection Act (“nFADP”);
  - (iii) all U.S. laws and regulations that apply to processing of personal data under the Agreement including but not limited to the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 - 1798.199)(“CCPA”);
  - (iv) all laws and regulations that apply to processing of personal data under the Agreement from time to time in place in the United Kingdom (including the UK GDPR); and
  - (v) the Personal Information Protection and Electronic Documents Act (“PIPEDA”), or any update, amendment or replacement of same that applies to processing of personal data in Canada.
  - The terms “controller”, “data protection impact assessment”, “process”, “processing”, “processor”, “supervisory authority” have the same meanings as in the GDPR or the UK GDPR.
  - The terms “Business”, “Business Purpose(s)”, “Commercial Purpose(s)”, “Personal Information”, “Service Provider”, “Sell”, and “Share” have the same meanings as defined in the CCPA.
- “SurveyMonkey” or “us” means in the case of Customers in the United States, SurveyMonkey Inc. and, in the case of customers outside of the United States, SurveyMonkey Europe.
- “SurveyMonkey Europe” means SurveyMonkey Europe UC, an Irish company, located at Ella House, Suite 40.4, 40 Merrion Square East, Dublin 2, D02 NP96, Ireland.
- “SurveyMonkey Inc.” means SurveyMonkey Inc., a Delaware corporation located at 910 Park Pl, Suite 300, San Mateo, CA 94403, United States.
- “SurveyMonkey Privacy Notice” means the SurveyMonkey Privacy Notice at <https://www.surveymonkey.com/mp/legal/privacy/>.

- "Personal Data" means information relating to a living individual who is, or can be, reasonably identified from the information, either alone or in conjunction with other information (a "Data Subject").
- "Services" means the services ordered by Customer from SurveyMonkey under the Agreement.
- "SCCs" 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 i)), the 5 February 2010 for the Transfer of Customer Personal Data to Processors established in Third Countries under Directive 95/46/EC). Where the nFADP applies, all references made in the SCCs shall be understood as corresponding references to the nFADP. All terms used in this context shall therefore receive the definition that is provided in the nFADP.
- "UK Addendum" means (i) the template addendum issued by the UK Information Commissioner's Office and laid before the UK Parliament in accordance with section 119A of the UK Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of the Mandatory Clauses from time to time. Where the template addendum referred to in this definition means the document entitled: International Data Transfer Addendum to the EU Commission Standard Contractual, version B1.0, in force 21 March 2022; or (ii) (until such time as SurveyMonkey has entered into the UK Addendum outlined at (i)), European Commission Decision of the 5 February 2010 for the transfer of personal data to processors established in third countries under Directive 95/46/EC.
- "UK GDPR" means the EU GDPR as it forms part of the laws of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020 respectively and any legislation in force in the United Kingdom from time to time that subsequently amends or replaces the UK GDPR.

## 2. Status of SurveyMonkey

In the provision of the Services to the Customer, SurveyMonkey is a processor of Customer Personal Data for the purposes of GDPR. With respect to CCPA, as applicable, SurveyMonkey and Customer hereby agree that SurveyMonkey is a Service Provider and Customer is the Business with respect to Personal Information.

## 3. Term

This DPA shall remain in force until such time as the Agreement is terminated (in accordance with its terms) or expires.

#### 4. Customer's Obligations

Customer shall ensure and hereby warrants and represents that it is entitled to transfer the Customer Data to SurveyMonkey so that SurveyMonkey may lawfully process and transfer the Personal Data in accordance with this DPA. Customer shall ensure that any relevant data subjects have been informed of such use, processing, and transfer as required by the Data Protection Legislation and that lawful consents have been obtained (where appropriate). Customer shall ensure that any Personal Data processed or transferred to SurveyMonkey will be done lawfully and properly. Customer will comply with all applicable Data Protection Legislation.

#### 5. SurveyMonkey's Obligations

Where SurveyMonkey is processing Customer Personal Data for Customer as a processor, SurveyMonkey will:

- (a) only do so on documented Customer instructions and in accordance with the Data Protection Legislation, including with regard to transfers of Customer Personal Data to other jurisdictions or an international organization, and the parties agree that the Agreement constitutes such documented instructions of the Customer to SurveyMonkey to process Customer Personal Data (including to locations outside of the EEA) along with other reasonable instructions provided by the Customer to SurveyMonkey (e.g. via email) where such instructions are consistent with the Agreement;
- (b) ensure that all SurveyMonkey personnel involved in the processing of Customer Personal Data are subject to confidentiality obligations in respect of the Personal Data;
- (c) make available information necessary for Customer to demonstrate compliance with its Article 28 obligations (or similar requirements in Data Protection Legislation 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 websites, provided that Customer provides SurveyMonkey with at least 14 days' written notice of such an information request;
- (d) co-operate 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;
- (e) provide assistance, when requested by the Customer, with requests received directly from a Data Subject in respect of a Data Subject's Personal Data submitted through the Services;
- (f) 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;

(g) 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;

(h) 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.

(i) not Sell or Share any Personal Information;

(j) not collect, retain, use, disclose, or otherwise process Personal Information other than for the following specific Business and Commercial Purposes: (1) to provide our Services as described in this Agreement; (2) to improve our existing services and develop new services (for example, by conducting research to develop new products or features); (3) for our operational purposes and the operational purposes of our vendors and integration partners; (4) to ensure security and integrity to the extent the use of the data subject's personal information is reasonably necessary and proportionate for these purposes; (5) Debugging to identify and repair errors that impair existing intended functionality; (6) Short-term, transient use, such as customizing content that we or our vendors display on the services; and (7) other uses that we notify you about as permitted under Data Protection Legislation;

(k) not retain, use, combine, or disclose the Personal Information collected pursuant to the Agreement outside the direct business relationship between SurveyMonkey and the Customer, unless expressly permitted by the CCPA;

(l) where required by Data Protection Legislation, inform Customer if it comes to its attention that any instructions received from the Customer infringe the provisions of Data Protection Legislation. Notwithstanding the foregoing, SurveyMonkey shall have no obligation to monitor or review the lawfulness of any instruction received from the Customer. If SurveyMonkey makes a determination that it can no longer comply with its obligations under the CCPA, SurveyMonkey will inform the Customer; and

(m) SurveyMonkey certifies that it understands the restrictions and obligations set forth in this DPA and all applicable Data Protection Legislation and that it will comply with those requirements.

## 6. Subprocessors

6.1 Subprocessing. Customer provides a general authorization to SurveyMonkey to engage onward subprocessors, subject to compliance with the requirements in this Section 6.

6.2 Subprocessor List. SurveyMonkey will, subject to the confidentiality provisions of the Agreement or otherwise imposed by SurveyMonkey:

- (a) make available to Customer a list of the SurveyMonkey subcontractors who are involved in processing or subprocessing Customer Personal Data in connection with the provision of the Services ("Subprocessors"), together with a description of the nature of services provided by each Subprocessor ("Subprocessor List"). A copy of this Subprocessor List may be reviewed [here](#);
- (b) ensure that all Subprocessors on the Subprocessor List are bound by contractual terms that are in all material respects no less onerous than those contained in this DPA; and
- (c) be liable for the acts and omissions of its Subprocessors to the same extent SurveyMonkey would be liable if performing the services of each of those Subprocessors directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6.3 New / Replacement Subprocessors. SurveyMonkey will provide Customer with written notice of the addition of any new Subprocessor or replacement of an existing Subprocessor at any time during the term of the Agreement ("New Subprocessor Notice"). The Customer will sign up to a mailing list made available by SurveyMonkey [here](#), through which such notices will be delivered by e-mail or alternatively will check on updates to the list [here](#). If Customer has a reasonable basis 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 Subprocessor Notice. In the event of such reasonable objection, either Customer or SurveyMonkey may terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the objected-to new Subprocessor (which may, at SurveyMonkey's discretion and election, involve termination of the entire Agreement) with immediate effect by providing written notice to the other party. Such termination will be without a right of refund for any fees prepaid by Customer for the period following termination.

## 7. Security

7.1 Security Measures. SurveyMonkey has, taking into account the state of the art, cost of implementation and the nature, scope, context and purposes of the Services and the level of risk, implemented appropriate technical and organizational measures (in accordance with Appendix 1) to ensure 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 ensuring the security of the processing.

7.2 Security Incident and Breach Notification. If SurveyMonkey becomes aware of any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Customer Personal Data ("Security Incident"), SurveyMonkey will take reasonable steps to

notify Customer without undue delay. 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. Any notification of a Security Incident to the Customer does not constitute any acceptance of liability by SurveyMonkey.

7.3 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.

## 8. Audits

8.1 Audits. Where SurveyMonkey is processing Customer Personal Data for Customer as a processor (only), the 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 subscription 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.
- (c) The scope of an audit will be limited to SurveyMonkey systems, processes, and documentation relevant to the processing and protection of Customer Personal Data, and Auditors will conduct audits subject to any appropriate and reasonable confidentiality restrictions requested by SurveyMonkey.
- (d) Customer will promptly notify and provide SurveyMonkey on a confidential basis with full details regarding any perceived non-compliance or security concerns discovered during the course of an audit.

8.2 The parties agree that, except as otherwise required by order or other binding decree of a supervisory authority or regulator with authority over the Customer, this Section 8 sets out the entire scope of the Customer's audit rights as against SurveyMonkey.

## 9. International Data Transfers

9.1 To the extent applicable, for transfers of Customer Personal Data from the European Economic Area ("EEA"), Switzerland, or the United Kingdom to locations outside the EEA, Switzerland, and the United Kingdom (either directly or via onward transfer) that do not have adequate standards of data protection as determined by the European Commission or relevant Data Protection Legislation, SurveyMonkey relies upon:

- (a) the SCCs; and
- (b) for transfers subject to the UK GDPR, the UK Addendum; or
- (c) such other appropriate safeguards, or derogations (to the limited extent appropriate), specified or permitted under the Data Protection Legislation.

9.2 Where required, the parties hereby enter into the SCCs (a copy of which is accessible [here](#)) and the UK Addendum (Appendix 3). The SCCs are incorporated into this Agreement by reference and shall apply as follows:

- (a) where Customer contracts with SurveyMonkey Inc. in the United States under the Agreement for Services and is a data controller of Customer Personal Data and through use of the Services is transferring that Customer Personal Data from the EEA to locations which have not been determined to provide adequate levels of protection to Personal Data by the European Commission, SurveyMonkey enters into the SCCs as data importer and the Customer enters into the SCCs as data exporter and Module Two only of the SCCs will apply; and/or
- (b) where Customer contracts with SurveyMonkey Inc. in the United States under the Agreement for Services and is a data processor of Customer Personal Data and through use of the Services is transferring that Customer Personal Data from the EEA to locations which have not been determined to provide adequate levels of protection to Personal Data by the European Commission, SurveyMonkey enters into the SCCs as data importer and the Customer enters into the SCCs as data exporter and Module Three only of the SCCs will apply; and/or
- (c) where Customer is not a resident of the EEA and contracts with SurveyMonkey Europe UC to store Customer Personal Data within the EEA under the Agreement, and is a data controller of Customer Personal Data, and through use of the Services is transferring that Personal Data from the EEA to locations which have not been determined to provide adequate levels of protection to Personal Data by the European Commission, SurveyMonkey enters into the SCCs as data exporter and the Customer enters into the SCCs as data importer and Module Four only of the SCCs will apply; and
- (d) in Clause 7, the optional docking clause will apply;
- (e) in Clause 9, option 2 will apply with a 15 day notice period;



- (f) in Clause 11, the optional language will not apply;
- (g) in Clause 17, the SCCs will be governed by Irish law;
- (h) in Clause 18, disputes shall be resolved before the courts of Ireland; and
- (i) Annex I and II of the SCCs shall be deemed completed with the information set out in the Agreement and details provided in the Appendices to this DPA.

9.3 For transfers that are protected by the nFADP, the SCCs shall apply in accordance with Section 9.2 above, except:

- (a) any references in the SCCs to the GDPR shall be interpreted as references to the nFADP;
- (b) any references to “EU”, “Union”, and “Member State law” shall be interpreted as references to Switzerland and Swiss law; and
- (c) any references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in Switzerland, unless the SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the nFADP, in which case the Swiss SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. For the purposes of the Swiss SCCs, the relevant Annexes of the Swiss SCCs shall be populated using the information contained in the Appendices I and II to this DPA (as appropriate) and the interpretive provisions set out in this section 9.3 shall apply (as applicable and as required for the purposes of complying with the nFADP).

9.4 Upon written request and in accordance with the provisions of the Standard Contractual Clauses or UK Addendum (as applicable), SurveyMonkey will provide copies of the Standard Contractual Clauses or UK Addendum that it has entered into with data importers in its capacity as processor to the Customer.

## 10. General Provisions

10.1 Liability for data processing. Each party's aggregate liability for any and all claims whether in contract, tort (including negligence), breach of statutory duty, or otherwise arising out of or in connection with this DPA shall be as set out in the Agreement, unless otherwise agreed in writing by the parties.

10.2 Conflict. In the case of conflict or ambiguity between: (i) the terms of this DPA and the terms of the Agreement, with respect to the subject matter of this DPA, the terms of this DPA shall prevail; (ii) the terms of any provision contained in this DPA and any provision contained in the Standard Contractual Clauses, the provision in the Standard Contractual Clauses shall prevail.

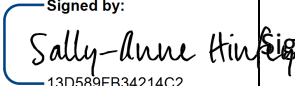
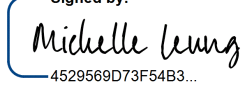
10.3 Independent Processing. Customer remains exclusively liable for its own compliance with Data Protection Legislation with respect to any independent collection and processing of personal data unrelated to the Services. Customer will provide its own clear and conspicuous privacy notices that accurately describe how it does this and SurveyMonkey will not be liable for any treatment of personal data by Customer in those circumstances. Customer hereby indemnifies SurveyMonkey in full for any and all claims or liability arising as a result of such collection and use of personal data by it in those circumstances.

10.4 Entire Agreement. The Agreement (which incorporates this DPA) and any Order Form represent the entire agreement between the parties and it supersedes any other prior or contemporaneous agreements or terms and conditions, written or oral, concerning its subject matter. Each of the parties confirms that it has not relied upon any representations not recorded in the Agreement inducing it to enter into the Agreement.

10.5 Severance. If any provision of this DPA 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. Nothing in this DPA is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, nor authorize any part to may or enter into any commitments for or on behalf of any other party except as expressly provided herein.

10.6 Electronic Copy. The DPA is delivered as an electronic document.

10.7 Governing Law. This DPA shall be governed by the laws of Ireland and the parties submit to the exclusive jurisdiction of the Irish courts (in relation to all contractual and non-contractual disputes) except in the case of any alleged breach or breach of current or future privacy laws, regulation, standards, regulatory guidance, and self-regulatory guidelines at state or federal level in the United States of America, in which case the laws of the State of California shall govern unless otherwise dictated by law.

Customer <sup>1</sup>	SurveyMonkey Europe UC	SurveyMonkey Inc.
Signature:	<div>Signed by: Signature:  13D589FB34214C2...</div>	<div>Signed by: Signature:  4529569D73F54B3...</div>
Name:	Name: Sally-Anne Hinfey	Name: Michelle Leung
Title:	Title: Vice President, Legal	Title: Senior Vice President, General Counsel & Secretary
Date:	Date: March 31, 2025	Date: March 31, 2025

<sup>1</sup> Note: this must be the person or organization named on the SurveyMonkey account (in the case of a person, they are acting in their capacity as an individual) NOT a related person or entity who is not party to the Agreement. If the party that signs here is not a party to an Agreement with SurveyMonkey this DPA will not be legally binding on SurveyMonkey.

## Appendix 1

### Description of the technical and organizational security measures implemented by SurveyMonkey

SurveyMonkey will maintain appropriate administrative, physical, and technical safeguards (“Security Safeguards”) for protection of the security, confidentiality and integrity of Customer 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 Customer Data are subject to confidentiality obligations.

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

(3) SurveyMonkey classifies the Customer Data it processes for Customer to help identify it and to allow for access to it to be appropriately restricted (e.g., through usernames, passwords, and encryption).

**(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.

(ii) 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.

(iii) 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.

(iv) Data Beyond Boundaries.

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

(v) 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.

**(f) 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.

**(g) 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.

**(h) Domain: Access Control to Processing Areas.**

- (i) 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:

- (1) establishing secure areas;
- (2) protection and restriction of access paths;
- (3) securing the mobile/cellular telephones;
- (4) data processing equipment and personal computers;
- (5) all access to the data centers where Customer Data are hosted is logged, monitored, and tracked;
- (6) the data centers where Customer Data are hosted is secured by a security alarm system, and other appropriate security measures; and
- (7) 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.

**(i) Domain: Access Control to Data Processing Systems.**

- (i) Processes to prevent data processing systems from being used by unauthorized persons, to include:
  - (1) identification of the terminal and/or the terminal user to the data processor systems;

- (2) automatic time-out after 30 minutes or less of user terminal if left idle, identification and password required to reopen;
- (3) issuing and safeguarding of identification codes;
- (4) password complexity requirements (minimum length, expiry of passwords, etc.); and
- (5) protection against external access by means of an industrial standard firewall.

**(j) Domain: Access Control to Use Specific Areas of Data Processing Systems.**

(i) 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 Data cannot be read, copied, modified or removed without authorization, to include by:

- (1) implementing binding employee policies and providing training in respect of each employee's access rights to the Customer Data;
- (2) effective and measured disciplinary action against individuals who access Customer Data without authorization;
- (3) release of data to only authorized persons;
- (4) implementing principles of least privileged access to information which contains Customer Data strictly on the basis of "need to know" requirements;
- (5) production network and data access management governed by VPN, two factor authentication, and role-based access controls;
- (6) application and infrastructure systems log information to centrally managed log facility for troubleshooting, security reviews, and analysis; and
- (7) 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.

**(k) Domain: Transmission Control.**

(i) Procedures to prevent Customer 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 Data by means of data transmission facilities is envisaged, to include:

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

- (2) implementation of VPN connections to safeguard the connection to the internal corporate network;
- (3) 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
- (4) monitoring of the completeness and correctness of the transfer of data (end-to-end check).

**(l) Domain: Storage Control.**

(i) When storing any Customer 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 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.

**(m) Domain: Input Control.**

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

- (1) authentication of the authorized personnel;
- (2) protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- (3) utilization of user codes (passwords);
- (4) proof established within data importer's organization of the input authorization; and
- (5) ensuring that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are locked.

**(n) Domain: Availability Control.**

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

**(o) Domain: Segregation of Processing.**

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

- (1) separating data through application security for the appropriate users;
- (2) storing data, at the database level, in different tables, separated by the module or function they support;
- (3) designing interfaces, batch processes and reports for only specific purposes and functions, so data collected for specific purposes is processed separately; and
- (4) barring live data from being used for testing purposes as only dummy data generated for testing purposes may be used for such.

**(p) Domain: Vulnerability management program.**

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

- (1) all networks, including test and production environments, regularly scanned; and
- (2) penetration tests are conducted regularly and vulnerabilities are remedied promptly.

**(q) Domain: Data Destruction.**

(i) 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:

- (1) all Customer Data shall be securely destroyed within 3 months; and
- (2) 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.

**(r) Domain: Standards and Certifications**

(i) 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.



**(s) Domain: Onsite Control.**

(i) When present on Customer's premises, all employees and subcontractors (if applicable) will comply with all reasonable rules, regulations, practices, and procedures (including, without limitation, security-related arrangements) generally prescribed by Customer and use Customer property only for the purposes set forth in an Agreement and will return all such property to Customer upon completing the applicable Services.

**(t) Domain: Data Quality Strategy.**

(i) SurveyMonkey implements a Data Quality Strategy designed to maintain data quality to an appropriate standard and corrects data when we are aware of incorrect or incomplete data by design. SurveyMonkey maintains cryptographic hashes of certain production data and change logs of domain data so we can monitor and track changes. We have processes in place for users to correct or withdraw processing of their personal information and also to correct data issues in the system.

(ii) SurveyMonkey collects accurate, relevant, and complete information from customers in order to enable their business operations.

(iii) SurveyMonkey maintains the Customer Data according to lifecycle policies in a timely fashion enabling consistent access to the data.

(iv) The standard for data quality may vary from customer to customer according to their use cases.

**(u) Domain: Privacy by Design.**

(i) SurveyMonkey has implemented policies and procedures to implement privacy by design. All Customer Data within the system is scoped according to appropriate access (by policy) and its lifecycle is maintained by policy. All systems connected to production have data minimization and pseudo anonymization as default, with a view towards preventing privacy and security issues rather than having to remediate them later.

(ii) We consider data protection issues part of the design and implementation of systems, services, products and business practices, and treat data privacy as a core function of our service.

(iii) We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.

(iv) We only process the Customer Data that we need for our purposes(s), and we only use Customer Data for those purposes.

(v) We ensure that Customer Data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy

(vi) We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

(vii) We use data processors that provide sufficient guarantees of their technical and organizational measures for data protection by design.

(viii) When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data privacy issues into account.

**(v) Domain: Testing of Data Security Posture.**

(i) SurveyMonkey will test its data security posture on an at least annual basis through pen testing through an industry standard tool (such as BurpScanner), or alternatively a certified third party service or consultant.

**(w) Domain: Data Loss Prevention Strategy.**

(i) SurveyMonkey uses training and education as a data loss prevention strategy. Access to data within the system is scoped and minimized to prevent users from having unneeded access to data. All users are required to sign policies about appropriate access to Customer Data, and this is part of the annual security refresher training.

**(x) Domain: Technical Security Measures.**

(i) SurveyMonkey is a distributed company so does not have any internal corporate firewalls or intrusion detection for our internal network. All access to corporate resources are to be done over encrypted channels. All corporate resources are required to be stored in MFA-enabled systems.

Appendix 2

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

The parties agree that the purpose and nature of the processing of Customer Personal Data, the types of personal data and categories of data subjects are as set out in this Appendix 2.

<b>Purposes and Nature of Processing</b>	<p>SurveyMonkey may process Customer Personal Data as necessary to technically perform the Services, including where applicable:</p> <ul style="list-style-type: none"><li>• Hosting and storage;</li><li>• Backup and disaster recovery;</li><li>• Technically improve the service;</li><li>• Service change management;</li><li>• Issue resolution;</li><li>• Providing secure, encrypted Services;</li><li>• Applying new product or system versions, patches, updates and upgrades; Monitoring and testing system use and performance;</li><li>• Proactively detect and remove bugs;</li><li>• IT security purposes including incident management;</li><li>• Maintenance and performance of technical support systems and IT infrastructure;</li><li>• Migration, implementation, configuration and performance testing; Making product recommendations;</li><li>• Providing customer support; transferring data, and</li><li>• Assisting with data subject requests (as necessary).</li></ul>
--	--

<p><b>Categories of Personal data</b></p>	<p>The Customer may submit Customer 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:</p> <ul style="list-style-type: none"> <li>• Personal data of all types that may be submitted by the Customer's respondents to the Customer via users 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.</li> <li>• 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).</li> <li>• 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.</li> </ul>
---	--

<p><b>Data Subjects</b></p>	<p>Data subjects include:</p> <ul style="list-style-type: none"> <li>• 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);</li> <li>• Natural persons whose personal data may be submitted to the Customer by Respondents via use of the Services;</li> <li>• Natural persons who are employees, representatives, or other business contacts of the Customer;</li> </ul>
-----------------------------	--

	<ul style="list-style-type: none"> <li>The Customer's users who are authorized by the Customer to access and use the Services.</li> </ul>
--	---

## ANNEXURES FOR Standard Contractual Clauses

### ANNEX I -

#### **A. LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): As stated in the Agreement

Contact person's name, position and contact details: As stated in the Agreement

Activities relevant to the data transferred under these Clauses: As stated in Appendix 2 of the DPA

Data importer(s): As stated in the Agreement

Name: As stated in the Agreement

Contact person's name, position and contact details: As stated in the Agreement

Activities relevant to the data transferred under these Clauses: As stated in Appendix 2 of the DPA

#### **B. DESCRIPTION OF TRANSFER**

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred: As stated in Appendix 2 of the DPA

Categories of personal data transferred: As stated in Appendix 2 of the DPA

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: As stated in Appendix 1 and 2 of the DPA

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): One-off and continuous (depending on use of Services)

Nature of the processing: As stated in Appendix 2 of the DPA

Purpose(s) of the data transfer and further processing: As stated in Appendix 2 of the DPA

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As stated in the Agreement and as stated [here](#)  
For transfers to (sub) processors, also specify subject matter, nature and duration of the Processing: [Please see here](#).

### **C. COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13: Ireland

ANNEX II – TECHNICAL AND ORGANIZATIONAL MEASURES AS STATED IN APPENDIX 1 OF THE DPA

ANNEX III – LIST OF SUBPROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

The Customer has authorized the use of the following subprocessors: [Please see here](#).

## Appendix 3

### United Kingdom

1. In relation to data transfers that are subject to the UK GDPR, the parties hereby enter into the UK Addendum (a copy of which is accessible [here](#)) and the UK Addendum is incorporated into this Agreement by reference. For data transfers that are subject to the UK GDPR, any references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the relevant data protection authority and courts in the UK.

2. The parties agree that the format and content of the tables in Part 1 of the UK Addendum shall be amended and replaced with the table below.

UK Addendum Table Reference	Information to complete the table
Table 1: Start date	Effective as of the Effective Date of the Agreement.
Table 1: Parties' details	Shall be deemed completed with the information set out in Appendix 2 of this Agreement.
Table 2: Addendum EU SCCs	<p>The parties select the following option from Table 2:</p> <p>"Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum".</p> <p>Details of the "modules", "clauses" and "optional provisions" of the SCCs that are brought into effect for the purposes of the UK Addendum are set out above in section 9.2 of this Agreement.</p>
Table 3: Annex 1A – List of parties	Shall be deemed completed with the information set out in Appendix 2 to this Agreement.
Table 3: Annex 1B – Description of Transfer	Shall be deemed completed with the information set out in Appendix 2 to this Agreement.
Table 3: Annex II – Technical and organizational measures	Shall be deemed completed with the information set out in Appendix 1 to this Agreement.
Table 3: Annex III: List of Sub processors (Modules 2)	A list of subprocessors can be found in accordance with the subprocessor provisions of the Agreement.
Table 4: Ending this Addendum	The parties select that neither party may end the UK Addendum as it is incorporated into the Agreement.

3. In the event of a conflict or inconsistency between this Agreement and the UK Addendum, the UK Addendum controls and take precedence in respect of such conflict or inconsistency.



## Appendix 4

### Australia

#### This Appendix

- 1) This appendix (**Appendix**) to the SurveyMonkey Data Processing Agreement (**DPA**) sets out the additional terms and conditions applicable to SurveyMonkey's Customers located in Australia, as well as the relevant obligations and requirements set out in the DPA.
- 2) Capitalised terms in this Appendix have the meaning given in the DPA, subject to the following terms which will apply to the DPA and this Appendix for Customers located in Australia:
  - a) **Eligible Data Breach** has the meaning given in the Privacy Act;
  - b) **Data Protection Legislation** has the meaning given in the DPA, subject to insertion of a new subclause to that definition, reading "the Privacy Act 1988 (Cth) ("**Privacy Act**")"; and
  - c) **Personal Data** means personal information, as defined in the Privacy Act, including information or opinion about an identified individual, or an individual who is reasonably identifiable.

#### SurveyMonkey's Obligations

- 3) In addition to SurveyMonkey's obligations under section 5 of the DPA, SurveyMonkey will comply with all applicable provisions of the Privacy Act (including in relation to the collection, use and disclosure of Personal Data).

#### Eligible Data Breaches

- 4) Section 7.1 of the DPA is deleted and replaced with:

**"7.1 Security Measures.** SurveyMonkey will, taking into account the cost of implementation and the nature, scope, context and purposes of the Services and the level of risk, implement appropriate technical and organisational measures (in accordance with Appendix 1) to ensure a level of security appropriate to the risk of unauthorised or unlawful access to or modification of Customer Personal Data. At reasonable intervals, SurveyMonkey will test and evaluate the effectiveness of these technical and organisational measures to ensure the security of the processing."

- 5) Section 7.2 of the DPA is deleted and replaced with:

**"7.2 Security Incident and Breach Notification.** If SurveyMonkey, become aware of any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or

destruction of, Customer Personal Data (“**Security Incident**”), SurveyMonkey will, in accordance with the relevant timeframes and requirements under the Privacy Act:

- (a) investigate, or procure the investigation of, the Security Incident;
- (b) assess if the Security Incident constitutes an Eligible Data Breach, and notify the Customer of whether:
  - (i) SurveyMonkey considers that a reasonable person would or would not conclude that the Security Incident is an Eligible Data Breach;
  - (ii) SurveyMonkey will make any statements to the affected individuals and the Office of the Australian Information Commissioner; and
  - (iii) where there are reasonable grounds to conclude that the Security Incident constitutes an Eligible Data Breach, SurveyMonkey will prepare statements in accordance with section 26WK of Part IIIC of the Privacy Act and make statements to the affected individuals and the Office of the Australian Information Commissioner to notify them of the Eligible Data Breach.
- (c) The parties otherwise take full responsibility for complying with their own obligations under the Privacy Act in respect of an Eligible Data Breach, and in respect of the Security Incident.”

### International Data Transfers

- 6) SurveyMonkey may transfer Customer Personal Data outside of Australia in accordance with the DPA, the Agreement, and our Privacy Policy.
  - a) SurveyMonkey will make all commercially reasonable endeavours to ensure its subprocessors comply with the Privacy Act, or are subject to law or binding scheme that have protections that are at least substantially similar to the way the Australian Privacy Principles under the Privacy Act protect the information.

### General

- 7) Section 10.1 of the DPA is deleted and replaced with:

**“10.1 Liability for data processing.** To the extent permitted by law, each party's aggregate liability for any and all claims whether in contract, tort (including negligence), breach of statutory duty, or otherwise arising out of or in connection with this DPA shall be as set out in the Agreement, unless otherwise agreed in writing by the parties.”
- 8) Notwithstanding section 10.2 of the DPA, this Appendix shall prevail over the terms of the DPA and the Agreement.

9) Section 10.4 of the DPA is deleted and replaced with:

**“10.4 Entire Agreement.** The Agreement (which incorporates this DPA and the Appendix) and any Order Form represent the entire agreement between the parties and it supersedes any other prior or contemporaneous agreements or terms and conditions, written or oral, concerning its subject matter. Each of the parties confirms that it has not relied upon any representations not recorded in the Agreement inducing it to enter into the Agreement.”

10) Section 10.7 (Governing Law) of the DPA is deleted and replaced with:

**“10.7 Governing Law** This DPA shall be governed by the laws of Victoria, Australia, and the parties submit to the exclusive jurisdiction of the courts of Victoria, Australia.”

## Explanatory Notes:

### Standard Contractual Clauses

We have drafted this DPA to include all possible SCC configurations. Not all of them may apply to you. For greater clarity:

- If you are an EU or UK Customer, you do not need SCCs, as you contract with SurveyMonkey's Irish entity, and no SCCs are needed between EU/UK entities.
- If you are a US Customer and consider yourself a data controller, Section 9.2(a) applies to you. You are the controller and the exporter, and SurveyMonkey is the processor and the importer. SCC Module 2 applies to your contract.
- If you are a US Customer and consider yourself a processor, Section 9.2(b) applies to you. You are the processor and the exporter, and SurveyMonkey is the (sub)processor and importer. SCC Module 3 applies to your contract.
- If you are not located in the US, EU, or UK, but you choose to use our EU data storage, Section 9.2(c) applies to you. You are the controller and the importer, and SurveyMonkey is the processor and exporter. SCC Module 4 applies to your contract.
- If you are **not** located in the US, EU, or UK and **do not** use our EU data storage, no SCCs are needed as personal data is transferred to SurveyMonkey Europe UC (located in Ireland). No transfer mechanism is needed for transfers into the EU.