DATA PROCESSING AGREEMENT

INTRODUCTION. The Data Processing Agreement ("***DPA***") forms part of the Agreement between Optimizely and Customer with respect to Customer's subscription to certain Software Services, and is the Parties' further agreement with regard to the Processing of Customer Data (including Personal Data). Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, on behalf of its Affiliates (as are Authorised User) and their respective personal Authorized-Users. To the extent that Optimizely Processes Personal Data in its provision of the Software Service, the Parties have agreed that Optimizely will do so on the terms of this DPA.

EFFECTIVE DATE: This DPA is effective on the Effective Date of the Agreement.

1. DEFINITIONS. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. For the purposes of this DPA only, and except where indicated otherwise, '*Customer*' shall include its Affiliates. The following definitons also apply-

1.1 "***Account Information***" means Customer's information, including Personal Data of Customer and Customer Affiliate's users, provided for account creation, access, administration, and maintenance, and may include names, usernames, login credentials, phone numbers, email addresses and billing information associated with an Optimizely account.

1.2 "***Controller***" means the entity (or person) which determines the purpose/s and mean/s of the Processing of Personal Data.

1.3 ***"Data Privacy Framework"*** means the EU-U.S. Data Privacy Framework, or where applicable, the UK Extension to the EU-U.S. Data Privacy Framework or the Swiss-U.S. Data Privacy Framework (all as detailed at https://www.dataprivacyframework.gov/s/).

1.4 "***Data Protection Laws***" means the laws (including regulations) applicable to the Parties' respective obligations for the Processing of Personal Data under this DPA.

1.5 "***Data Subject***" means the identified or identifiable person to whom Personal Data relates.

1.6 "***EEA***" means the European Economic Area.

1.7 "***ePHI-Enabled Software Service***" means those Software Services that Optimizely makes available for Subscription that may be Used by Customer for ePHI Processing.

1.8 **"*Exhibit* 2**" means Exhibit 2 and 2A.

1.9 "***GDPR***" means **(i)** the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and **(ii)** the UK GDPR (as defined in the Data Protection Act 2018), as the case requires.

1.10 "***HIPAA***" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as modified by the Health Information Technology for Economic and Clinical Health (HITECH) Act (Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5)), and the Secretary of HHS issued regulations at 45 C.F.R. Parts 160 and 164, as the same may be amended from time to time, and amendments and modifications, including any that are subsequently adopted.

1.11 "***Mandatory Clauses***" means 'Part 2: Mandatory Clauses' of the UK Addendum.

1.12 "***Optimizely***" means the Optimizely Group company as set out in the Order Form.

1.13 "***Optimizely Group***" means Optimizely and its Affiliates.

1.14 "***Personal Data***" means any Customer Data **(i)** relating to an identified or identifiable natural person and/or **(ii)** which is otherwise protected as personal data, personal information, personally identifiable information (or similar) under Data Protection Laws - but it excludes Personal Data contained in Account Information.

1.15 "***Processing***" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.16 "***Processor***" means the entity that Processes Personal Data on behalf of the Controller.

1.17 "***Sensitive Information***" means any Personal Data that is defined as sensitive information (or data) under applicable Data Protection Laws, and as such accordingly requires additional protections, safeguards or security measures under such applicable laws. Sensitive Information includes, but is not limited to, ePHI, and Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences.

1.18 "***Standard Contractual Clauses***" or "***SCCs***" means the standard contractual clauses for the transfer of personal data to processors pursuant to the European Commission's decision (EU) 2021/914 - either Module Two (controller to processor) or Module Three (processor to processor) of the Standard Contractual Clauses - as set out in **Exhibit 2** and **Exhibit 2A,** as may be applicable, as may be updated from time to time in accordance with the applicable Data Protection Law – and where the Data Protection Law are the laws of the United Kingdom, Standard Contractual Clauses shall include the UK Addendum.

1.19 "***Sub-processor***" means any Processor engaged by Optimizely or a member of the Optimizely Group.

1.20 "***Supervisory Authority***" means an independent statutory regulatory authority with respect to Personal Data privacy under applicable Data Protection Laws.

1.21 "*Third Country*" means any country, organization or territory not acknowledged under applicable Data Protection Laws as a safe country with an adequate level of data protection.

1.22 "*TOMs*" means Optimizely's technical and organizational security measures as outlined in Section 3.2 below.

1.23 "*UK Addendum*" means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK Parliament on 2 February 2022, a true copy of which is set out in Exhibit 3A, as completed, as revised in accordance with section 18 of the Mandatory Clauses as set out in Section 9.3 below.

1.24 "*US Data Protection Law*" means, to the extent applicable, federal and state laws relating to data protection, the Processing of Personal Data, privacy and/or data protection in force from time to time in the United States.

The terms "*Business Associate*", "*Covered Entity*", "*Protected Health Information*", "*PHI*" "*Electronic Protected Health Information*" and "*ePHI*" have the meanings ascribed under HIPAA. "*BAA*" means a Business Associate contract meeting the requirements of HIPAA.

2. PROCESSING OF PERSONAL DATA

2.1 *Roles of the Parties*. As between the Parties -

2.1.1 For the purposes of the GDPR, Optimizely acts as "Processor" or "Sub-processor" - as determined by the function of Customer. In general, Customer functions as a Controller, whereas Optimizely functions as a Processor. However, In certain cases, Customer functions as a Processor on behalf of Customer's customers where Customer and Customer's customer have concluded a data processing agreement in relation to the Processing of Personal Data of Customer's customers.

2.1.2 For the purposes of US Data Protection Law, Optimizely acts as a service provider, contractor and /or processor in its performance of its obligations pursuant to the Agreement.

2.2 *Account Information*. Account Information shall not be governed by this DPA and shall be subject to the Optimizely Privacy Notice.

2.3 *Optimizely's Processing.* Optimizely shall only Process Personal Data in accordance with Customer's documented instructions for the following purposes: **(i)** Processing in accordance with the Agreement and applicable Order; **(ii)** Processing initiated by Users in their Use of the Software Services; and **(iii)** Processing to comply with other documented reasonable instructions provided by Customer (including but not limited to email) where such instructions are consistent with the terms of the Agreement. Optimizely will Process Personal Data in accordance with the requirements under applicable Data Protection Law directly applicable to Optimizely's provision of its Software Service. For ePHI-Enabled Software Services and ePHI Processing by Optimizely as a Business Associate, Optimizely will enter into a Business Associate Agreement with the Customer. Optimizely shall be entitled to Process Personal Data in countries acknowledged by the European Union based on Article 45 of GDPR as a safe country with an adequate level of data protection, including the United Kingdom and the United States, as well as Third Countries outside the EU/EEA, including, in particular, (but without limitation) Vietnam, Bangladesh and Australia for support purposes. Upon request, Optimizely shall provide Customer with updates to its countries where Software Service support are located. Optimizely Group may engage third-party Sub-processors in accordance with the requirements set out in **Annex III** of the Appendix to **Exhibit 2**. For ePHI-Enabled Software Services, Optimizely will ensure it has Business Associate Agreements with its Sub-processors.

2.4 *Customer's Personal Data Obligations.* Customer shall, in its Software Services Use and instructions under this DPA with respect to the Processing of Personal Data by Optimizely ensure for its benefit its compliance with applicable Data Protection Laws, and has the responsibility for: **(i)** the accuracy, quality, and legality of Personal Data, and the means by which Customer acquired Personal Data, including but not limited to the proper notice and consent required for such Personal Data; **(ii)** ensuring that any transfers of Personal Data to third parties (other than Optimizely Group and its Sub-processors) ("**Customer Third Parties**") (such as Customer shared-services Affiliates, or Third-Party applications or platforms that Customer utilises in its Use of the Software Services) which either **(A)** are enabled through accounts or connections set up and deployed by Customer when Using the Software Services, or **(B)** enabled by accounts or connections set up by Optimizely pursuant to Customer's instructions, comply in both cases with Data Protection Laws; **(iii)** determining the Personal Data it transfers or instructs Optimizely to transfer; and **(iv)** assessing which Data Protection Laws apply to such transfer; and the selection and the terms of engagement of third-party transferees (including any assessment of the requirement for, and the sufficiency of, supplementary safeguard measures to ensure the protection of the Personal Data transferred in the country to which it is to be imported).

2.5 *Customer Third Parties.* Further to Section 2.4 (ii) above, Customer acknowledges that Optimizely (as Processor) has no contractual (or other) relationship with those Customer Third Parties or any rights of oversight or control over them or their Processing operations which may change from time to time and that it is, therefore, reasonable that Customer should have that responsibility for such compliance. Accordingly, Customer should ensure that any Control or Processing by Customer Third Parties of such Personal Data by those Customer Third Parties also complies with applicable Data Protection Laws, and Customer shall inform Optimizely without unreasonable delay should it become aware that any transfer by Optimizely of such Personal Data no longer complies with Data Protection Laws, in which case Optimizely shall be entitled to discontinue such transfers (to Customer Third Parties), and Customer shall promptly take such measures as are required to remedy such non-compliance.

2.6 *Details of the Processing.* The subject-matter of Processing of Personal Data by Optimizely is with respect to its delivery of the Software Services to Customer. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in **Exhibit 1**.

2.7 *Contrary Processing Instructions*. If Customer's instructions will cause Optimizely to Process Personal Data in violation of applicable Data Protection Law or outside the scope of the Agreement or the DPA, Optimizely shall promptly inform Customer, unless prohibited by applicable Data Protection Law (without prejudice to the SCCs).

3. OBLIGATIONS OF PROCESSOR

3.1 *Optimizely Resources, Personnel, and Employees*

3.1.1 Confidentiality. Optimizely shall ensure that its personnel engaged in the Processing of Customer Data are informed of the confidential nature of Customer Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Optimizely shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

3.1.2 Reliability. Optimizely shall take commercially reasonable steps to ensure the reliability of any Optimizely personnel engaged in the Processing of Customer Data.

3.1.3 Assistance. Optimizely shall provide reasonable assistance and co-operation in response to any request in writing by Customer to assist Customer to comply with its obligation to ensure that such transfers can be made in accordance with Data Protection Laws.

3.1.4 Limitation of Access. Optimizely shall ensure that Optimizely's access to Customer Data is limited to those personnel performing Services in accordance with the Agreement.

3.1.5 Data Protection Officer. Each entity that comprises the Optimizely Group has appointed a data protection officer. The appointed person may be reached at dpo@optimizely.com.

3.2 *Security Controls*

3.2.1 Technical and Organizational Measures. Optimizely shall maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of the Customer Data. ("**TOMs**"), Optimizely's TOMS are published (and as updated from time to time at: https://www.optimizely.com/trust-center/privacy/toms/).

3.2.2 Maintenance Program. Optimizely maintains a formal program to maintain the TOMs and respond to emerging risks, changes in applicable legal requirements, technical and organizational changes. Optimizely regularly monitors the effectiveness and compliance with the TOMs.

3.2.3 Updates. The TOMs are subject to update from time to time for purposes of continuous improvement. Comparable or better levels of security will be maintained. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

3.2.4 Controls and Auditing. Optimizely routinely audits its TOMs to assure effectiveness and evidence of continual use. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Optimizely shall make available to Customer (or Customer's independent, third-party auditor) documentation and other evidence of the effectiveness of the controls, as applicable, subject to the safeguarding of Optimizely's legitimate interests and to the extent commercially feasible. Optimizely may decline to provide internal documentation to its competitors (whether this includes Customer or an auditor).

3.3 *Customer Data Incident Management and Notification*

3.3.1 Notice. Optimizely shall notify Customer, without undue delay, and in no case more than twenty-four (24) hours of a confirmed accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, transmitted, stored, or otherwise Processed by Optimizely or its Sub-processors. ("***Security Incident***").

3.3.2 Identify, Remediate and Inform. Upon a Security Incident, Optimizely shall promptly: **(i)** make all reasonable efforts to identify the cause of such Security Incident, **(ii)** take those steps as Optimizely deems necessary and reasonable in order to remediate the cause of such that Security Incident to the extent the remediation is within Optimizely's reasonable control, **(iii)** provide Customer with all such information as Customer reasonably requests in connection with such incident, **(iv)** take such steps as Customer reasonably requires it to take to mitigate the detrimental effects of any such Security Incident on any Data Subjects in relation to their Personal Data, and/or on Customer, and **(v)** otherwise co-operate with Customer in investigating and dealing with such Security Incident. Optimizely's obligations in this Section 3.3.2 shall not apply to security incidents caused by Customer or any Authorized User. Optimizely's notification of, or response to, a Security Incident under this 3.3.2 will not be construed as an acknowledgment by Optimizely of any fault or liability with respect to the Security Incident.

3.4 *Deletion and/or Return of Customer Data*

3.4.1 Deletion and/or Return. On Customer's request or no later than thirty- five (35) days after the end of access to the Software Service upon expiration or the earlier termination of the Agreement, Optimizely will to the extent allowed by applicable law, permanently destroy all copies of Personal Data in its possession (in any form or format whatsoever) using industry standard data-destruction methods from all Optimizely-controlled storage. On the Customer's request, data shall be returned to the Customer in an industry standard format mutually agreed by the Parties. Any additional cost for reformatting will be borne by the Customer.

4. OBLIGATIONS OF CONTROLLER

4.1 ***Data Protection Laws.*** Customer shall comply with its obligations as Controller in relation to its Processing of the Personal Data under Data Protection Laws.

4.2 ***Updating Optimizely.*** Customer shall inform Optimizely without undue delay and comprehensively about any errors or irregularities related to the Processing of Personal Data detected or if it identifies any Personal Data being Processed in its use of the Software Services that contravenes Section 5 below and, where required by Optimizely to do so, shall promptly take such steps as Optimizely may require to bring its use of the Software Services into conformance with Section 2.1.

4.3 ***Implementation.*** Optimizely provides the core Software Service, which Customer is then responsible for implementing (which may include, but is not limited to, customizing, and configuring the base Software Services) ("***Implementation***"). Optimizely will not have any responsibility or liability that may result from Customer's Implementation.

5. RESTRICTIONS

5.1 ***Software Services Restrictions.*** The features, functions, capabilities and restrictions of the Software Services are described in the applicable Service Descriptions. The Service Descriptions may specify whether Personal Data Processing is permitted, and /or whether there are applicable restrictions. Where a Service Description does not permit, or restricts, Personal Data Processing, Customer shall not Process Personal Data within the relevant Software Service, unless as permitted in the Service Description.

5.2 ***Sensitive Information.*** Except with respect to ePHI-Enabled Software Service Subscription by Customer, notwithstanding anything to the contrary in any Service Description, the Software Services are not otherwise intended to Process Sensitive Information. Customer is solely responsible for determining whether Using the Software Service to Process its Sensitive Information complies with Data Protection Laws. If Customer uploads Sensitive Information in its Use of the Software Service for Optimizely Processing, Customer is acknowledging that Optimizely's TOMs are sufficient and satisfactory for its purposes in relation to that Processing of its Sensitive Information.

6. DATA SUBJECT RIGHTS

6.1 ***Data Subject Request.*** As between the Parties, Customer has sole discretion and responsibility in responding to the rights asserted by any individual in relation to Personal Data ("**Data Subject Request**" or "**DSR**"). Optimizely will promptly forward to Customer any Data Subject Request received by Optimizely or its Sub-processors from an individual in relation to Personal Data. Optimizely may advise the individual to contact Customer directly in relation to the Data Subject Request.

6.2 ***DSR Assistance.*** Taking into account the nature of Optimizely's Processing of Personal Data, Optimizely will provide Customer with self-service functionality through the Software Services or other reasonable assistance as necessary for Customer to meet its obligations under Data Protection Laws to respond to Data Subject Requests.

6.3 ***Incomplete and Duplicate DSRs.*** Customer must ensure that it does not send to Optimizely incomplete or duplicative assistance requests in relation to Data Subject Requests.

6.4 ***Software Service Only.*** Optimizely shall only be obliged to provide assistance in relation to Data Subject Requests where the Personal Data is Processed by Optimizely, and any such obligation does not extend to any Personal Data Processed outside of the Software Service.

7. DPA AUDITS

7.1 ***Audit Rights.*** Customer may subject to the confidentiality obligations under the Agreement, exercise the audit rights set out in this Section 7 in order to review the TOMs maintained by Optimizely as it relates to Processing within Customer's Software Service. Customer may appoint an independent third-party auditor (that is not a competitor of Optimizely) ("***Auditor***") to conduct its audit rights under this Section 7. Customer will document the resulting audit findings and provide Optimizely an opportunity to document any inconsistencies.

7.2 ***Examination of Optimizely Information.*** Optimizely will make available to Customer, upon request and subject to Section 7.1, information necessary to demonstrate compliance with its processing obligations. This information includes the most recent reports, certificates and/or extracts ("**Information**") prepared by an independent auditor. Information includes industry-accepted audit documents such as SOC 2 and ISO reports. Information also includes information pertaining to Optimizely's evaluation of Sub-processors. The Parties acknowledge that Customer's review of Information provided by Optimizely will be used as input to the Customer's audit requirements and reduce the need or scope of a more detailed Audit under Section 7.3 below.

7.3 ***Audit.*** If the Examination of Optimizely Information set out in Section 7.2 above does not provide, in Customer's reasonable judgment, sufficient evidence to confirm Optimizely's compliance with the terms of this DPA, then Customer may conduct a more detailed audit ("**Audit**"). This Audit is subject to the following conditions:

7.3.1 Requirements. The Audit will be subject to the requirements set out above in Section 7.1;

7.3.2 Limit. Customer may not Audit Optimizely more than once annually (unless otherwise required by government regulator or Supervisory Authority or triggered by a Security Incident) and the scheduling of the Audit will be mutually agreed at least sixty (60) days in advance of an Audit start date;

7.3.3 Plan. Customer will submit a detailed audit plan ("**Audit Plan**") at least ten (10) business days in advance and be mutually agreed by the Parties at least five (5) business days in advance of the scheduled Audit date – any delay may require a re-scheduling of the Audit;

7.3.4 Business Hours. The Audit will be conducted during regular business hours and without interrupting Optimizely's business operations; Customer's Audit expenses will be at Customer's sole cost; and

7.3.5 Restriction. If Customer's current total yearly spend with Optimizely is less than US$30,000 dollars per year, the Audit will be subject to prior agreement between the Parties to cover Optimizely's costs for preparation and participation in the Audit on a professional services basis.

7.4 ***GDPR.*** None of the conditions for the Audit in Section 7.3 limit any audit rights set out in Article 28 of GDPR.

8. SUB-PROCESSORS

8.1 ***Appointment of Sub-processors***. Customer acknowledges and agrees that **(a)** Optimizely's Affiliates may be retained as Sub-processors; and **(b)** Optimizely and Optimizely's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Software Services. Optimizely or a Optimizely Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations no less protective than those in this DPA and Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Software Services provided by such Sub-processor and complies with Data Protection Laws (including the regulations applicable to the transfers of personal data to Third Countries according to GDPR Articles 44-50). Where such an engagement will involve the transfer of Personal Data to a Third Country, the Customer agrees and acknowledges that Optimizely shall be entitled to leverage Standard Contractual Clauses for processor to processor transfers. Controller hereby authorizes Optimizely to conclude such Standard Contractual Clauses with the relevant Sub-contractors domiciled in Third Countries.

8.2 ***List of Current Sub-processors and Notification of New Sub-processor***. The current list of Sub-processors is made available by Optimizely on Optimizely's Trust Center Resources webpage (also accessible via https://www.optimizely.com/trust-center/privacy/sub-processors/). Optimizely shall provide Notification of a new Sub-processor before authorizing any new Sub-processor to Process the Customer's Customer Data. Such Notification is provided at https://status.optimizely.com/ and functionality for subscription is available on the web page.

8.3 ***Objection Right for New Sub-processors***. Customer may object to Optimizely's use of a new Sub-processor by notifying Optimizely promptly in writing within thirty (30) days after receipt of Optimizely's notice in accordance with the mechanism set out in the Agreement. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Optimizely will use reasonable efforts to make available to Customer a change in the Software Services or recommend a commercially reasonable change to Customer's configuration or use of the Software Services to avoid Processing of Customer Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Optimizely is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Agreement and/or Order(s) with respect only to those Software Services which cannot be provided by Optimizely without the use of the objected-to new Sub-processor by providing written notice to Optimizely. Optimizely will refund any pre-paid, unused fees following the effective date of termination with respect to such terminated Software Service.

8.4 ***Liability***. Optimizely shall be liable for the acts and omissions of its Sub-processors to the same extent Optimizely would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

9. INTERNATIONAL TRANSFERS

9.1 ***Data Privacy Framework.*** Optimizely North America Inc. has self-certified under the Data Privacy Framework and has agreed as a condition of its certification with the applicable data privacy principles. Details of Optimizely's certification is available at https://www.dataprivacyframework.gov/list. [Search for Optimizely]. To the extent the Data Privacy Framework is acknowledged as a valid transfer mechanism in the relevant territory, Customer's Personal Data originating from the EEA (or, as applicable, from the UK or Switzerland) shall be transferred to the United States on the basis of that Data Privacy Framework.

9.2 ***Standard Contractual Clauses***. Module Two and /or Module Three shall apply with respect to transfers of Personal Data to a Third Country, either directly or via onward transfer, not otherwise covered by a suitable framework recognized under applicable Data Protection Law as providing an adequate level of protection for Personal Data, including binding corporate rules for processors. The Modules are subject to Section 9.3 below.

9.3 *SCC Elections and Amendments*

Relevant SCC Clause	Application
Clause 7 - the Docking Clause)	Does not apply.
Clause 9(a) - *General written authorization*	Selected. The time period to be specified is determined in clause 8.3 of the DPA
Clause 11(a) - *Independent dispute resolution body*	Does not apply.
Clause 17 - *Governing law*	Option one applies. The Parties agree to submit themselves to the jurisdiction of the courts of Sweden.
Clause 18 - *Forum and Jurisdiction*	The Parties agree to submit themselves to the jurisdiction of the courts of Sweden.
Annex I	Exhibit 1 contains the specifications regarding the Parties, the description of transfer, and the competent supervisory authority.
Annex II	Section 3.2 of this DPA outlines the technical and organizational measures for protection of the security, confidentiality and integrity of the Personal Data. Optimizely's technical and organizational measures are published at: https://www.optimizely.com/trust-center/privacy/toms/).
Annex III	Clause 8.1 of the DPA applies. The Sub-processor's contact person's name, position and contact details will be provided by Optimizely upon request.

9.3.1 Where applicable Data Protection Law adopts the updated or new Standard Contractual Clauses as meeting required adequacy means as an alternative to, or update of, the applicable Standard Contractual Clauses, then those updated Standard Contractual Clauses shall apply in lieu of those prior Standard Contractual Clauses (subject always to the elections in this Section 9.3 above).

9.4 ***Personal Data Subject To UK Data Protection Law.*** With respect to any transfers of Personal Data falling within the scope of the UK GDPR from Customer (as data exporter) to Optimizely (as data importer), the UK Addendum (set out in **Exhibit 3A**) shall form part of this DPA, and the Standard Contractual Clauses shall be read and interpreted in light of the provisions of the UK Addendum, to the extent necessary according to clause 12 of the Mandatory Clauses (of that UK Addendum).

9.5 *UK Addendum Deviations, Elections and Amendments*

9.5.1 Table 1 of the UK Addendum has been completed in **Exhibit 3A** with details of the Parties..

Relevant UK Addendum Clause or Table	Application
Selected Modules	As specified in Table 2 of **Exhibit 3A**. For reference - Module Two (Controller to Processor) and Module Three (Processor to Processor).
Table 2 / Clause 7 – Docking Clause	As specified in Section 9.3 (*SCC Elections and Amendments*) above, as amended by the Mandatory Clauses.
Table 2 / Clause 9a – *Prior Authorisation or General Authorisation*	As specified in Section 9.3 (*SCC Elections and Amendments*) above, as amended by the Mandatory Clauses.
Table 2 / Clause 9a – Time Period	As specified in Section 9.3 (*SCC Elections and Amendments*) above, as amended by the Mandatory Clauses.
Clause 12 of the Mandatory Clauses - *Forum and Jurisdiction*	The UK Addendum (including the applicable SCCs) is governed by the laws of England and Wales, any dispute arising from it is resolved by the courts of England and Wales.
Clause 16 of the Mandatory Clauses - laws of Scotland and Northern Ireland	Does not apply.

9.6 ***Personal Data Subject To Swiss Data Privacy Laws.*** To the extent that the processing of Personal Data is subject to Swiss Data Protection Law, the Swiss Addendum (set out in **Exhibit 3B)** shall apply.

9.7 *Swiss Addendum, Elections, Amendments and Notices*

9.7.1 Switzerland. The Swiss Addendum shall be governed by the laws of Switzerland insofar as the transfers are governed by Data Protection Law of Switzerland.

9.7.2 Other Legal Persons. Until the entry into force of the revised Swiss Data Protection Laws, the Clauses shall also protect personal data of legal entities, and legal entities shall receive the same protection under the Clauses as natural persons.

9.7.3 Switzerland & GDPR. To the extent that any Processing of Personal Data is subject to both Swiss Data Protection Laws and the GDPR, the DPA (including the Clauses as further specified in Section 9.3 above) will apply as is, and additionally, to the extent that a transfer is subject to Swiss Data Protection Law, as amended by clauses I, II, IV & V of the Swiss Addendum, with the sole exception that clause 17 of the SCCs shall not be replaced as stipulated under clause V.8 of the Swiss Addendum.

9.7.4 Affiliates. Customer warrants that it and/or Customer Affiliates have made all relevant notifications to the Federal Data Protection and Information Commissioner (FDPIC) which are required under Swiss Data Protection Laws.

9.8 ***Personal Data Subject To US Data Privacy Laws.*** To the extent that the processing of Personal Data is subject to US Data Protection Laws, the U.S. Addendum (set out in **Exhibit 3C**) shall apply.

9.9 ***Supplementary Measures***. Optimizely further agrees to implement the supplementary measures set forth in **Exhibit 4** of this DPA so as to facilitate Customer's compliance with requirements that may be additionally imposed (on the Customer) with respect to Customer Data Processing (including transfers of Personal Data to Third Countries).

10. DUTIES TO INFORM, MANDATORY WRITTEN FORM, CHOICE OF LAW, ADDITIONAL TERMS

10.1 ***Search.*** Where Customer's Customer Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed, Optimizely shall inform Customer without undue delay unless legally prohibited. Optimizely shall, without undue delay, notify to all pertinent parties in such action, that any Customer Data affected is in Customer's sole property and area of responsibility, that Customer Data is at Controller's sole disposition, and that Controller is the responsible body with respect to relevant Personal Data in the sense of Data Protection Laws.

10.2 ***DPA Updates.*** Where updates to this DPA are required or are appropriate as a result of any changes to the requirements of Data Protection Laws, Optimizely shall be entitled to amend this DPA upon giving Customer at least ninety (90) days' prior written notice. Upon Customer's receipt of Optimizely's notice, Optimizely and Customer will work together in a timely manner and in good faith to agree upon, and to document any such necessary DPA updates.

10.3 ***Multiple Transfer Mechanisms.*** In the event that the Software Service is covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: **(1)** the Data Privacy Framework; and **(2)** the Standard Contractual Clauses. The transfer mechanisms referenced in this Section 10.3 are made available to apply to transfers of Personal Data subject to the restrictions and controls contemplated under this DPA and, in particular, but without limitation, on the basis that Customer shall comply with the terms of this DPA.

10.4 ***Invalidities.*** Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

10.5 ***BAA and DPA Conflict.*** If the Agreement also includes a Business Associate Agreement, any conflict between the provisions of this DPA and that Business Associate Agreement with respect to Optimizely's Processing of Customer Data and Customer's rights and obligations in relation thereto, the provisions of the Business Associate Agreement will control solely with respect to Optimizely's Processing of ePHI in an ePHI-Enabled Software Service.

10.6 **Data Protection Transfer Impact Assessment.** Optimizely will provide Customer reasonable support to enable Customer's compliance with the requirements imposed on the transfer of Personal Data to Third Countries with respect to Data Subjects located in the EEA, Switzerland, and UK. Optimizely will, upon Customer's reasonable request, provide information to Customer which is reasonably necessary for Customer to complete a transfer impact assessment ("**TIA**"). Optimizely may charge Customer, and Customer shall reimburse Optimizely, for any assistance provided by Optimizely with respect to any TIAs, data protection impact assessments or consultation with any Supervisory Authority of Customer. Optimizely's obligation to assist is subject to Customer not otherwise having access to the relevant information, and to the extent such information is available to Optimizely. Optimizely shall also provide commercially reasonable assistance to Customer in its cooperation or any consultation with the applicable Supervisory Authority with respect to its assistance to Customer in its TIA to the extent required under applicable Data Protection Law.

EXHIBITS:

- Exhibit 1: Details of the Processing
- Exhibit 2: Standard Contractual Clauses (Module Two) [(Controller to Processor)]
- Exhibit 2A: Standard Contractual Clauses (Module Three) [(Processor to Processor)]
- Exhibit 3A: UK Addendum to the EU Commission Standard Contractual Clauses
- Exhibit 3B: Swiss Addendum to the EU Commission Standard Contract
- Exhibit 3C: US Data Protection Law Addendum
- Exhibit 4: Supplementary Measures