

INTRODUCTION

The Data Processing Agreement (“*DPA*”) forms part of the Agreement between Optimizely and Customer for purchase of subscriptions to Software Services, and is the parties’ further agreement with regard to the Processing of 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 to the extent Optimizely processes Personal Data for which such Affiliates act as Controllers.

For the purposes of this DPA only, and except where indicated otherwise, “*Customer*” shall include its Affiliates.

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

Terms of the DPA

1. DEFINITIONS

- 1.1 “*Optimizely*” means the Optimizely Group company as set out in the Order Form.
- 1.2 “*Optimizely Group*” means Optimizely and its Affiliates.
- 1.3 “*Controller*” means the entity which determines the purposes and means of the Processing of Personal Data.
- 1.4 “*Data Privacy Framework*” means the EU-US Data Privacy Framework, or where applicable, the UK Extension to the EU-US Data Privacy Framework or the Swiss-US Data Privacy Framework (all as detailed at <https://www.dataprivacyframework.gov/s/>).
- 1.5 “*Data Protection Laws*” means the laws (including regulations) applicable to the parties’ respective obligations for the Processing of Personal Data under this DPA.
- 1.6 “*Data Subject*” means the identified or identifiable person to whom Personal Data relates.
- 1.7 “*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.
- 1.8 “*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.
- 1.9 “*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.
- 1.10 “*Processor*” means the entity which Processes Personal Data on behalf of the Controller.
- 1.11 “*Sensitive Information*” means any Personal Data that is defined as sensitive information or sensitive data under applicable Data Protection Laws and that requires additional protections, safeguards or security measures under such applicable laws. Sensitive Information includes, but is not limited to, 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.
- 1.12 “*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 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 relevant the Data Protection Law are the laws of the United Kingdom, *Standard Contractual Clauses and SCCs* shall be interpreted to include any standard data protection clauses adopted under UK GDPR, Art.46.
- 1.13 “*Sub-processor*” means any Processor engaged by Optimizely or a member of the Optimizely Group.
- 1.14 “*Supervisory Authority*” means an independent statutory regulatory authority with respect to Personal Data privacy under applicable Data Protection Laws.
- 1.15 “*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.
- 1.16 “*TOMs*” means Optimizely’s technical and organizational security measures as outlined in section 3.2 below.

2. PROCESSING OF PERSONAL DATA

2.1 *Roles of the Parties.* As between the parties, Customer is the Controller and Optimizely is the Processor with respect to the Personal Data Processing. Optimizely Group may engage third-party Sub-processors in accordance with the requirements set out in **Annex III** of the **Appendix** to **Exhibit 2** and **Exhibit 2A**.

2.2 *Compliance.* Customer, as Controller, is solely responsible for its compliance with its Data Protection Laws with regard to any Processing of Personal Data under this DPA, including transfers of Personal Data which occur in contravention of Section 5 below or because required supplementary measures were not implemented as a result of a failure by Customer to notify Optimizely of the requirement for them.

2.3 *Optimizely's Processing.* Personal Data is Customer Confidential Information, and the confidential obligations of the Agreement apply to that Personal Data. 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 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.

2.4 *Customer's Processing of Personal Data.* Customer shall, in its Software Services Use, Process Personal Data in accordance with the requirements of Data Protection Laws. Customer's instructions for the Processing of Personal Data must comply with Data Protection Laws. Customer shall have sole responsibility for -

2.4.1 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;

2.4.2 ensuring that any transfers of Personal Data to third parties (other than Optimizely Group and Sub-processors) which either **(i)** are enabled through accounts or connections set up and deployed by Customer when using the Software Services, or **(ii)** enabled by accounts or connections set up by Optimizely pursuant to Customer's instructions, comply with Data Protection Laws;

2.4.3 determining the Personal Data it transfers or instructs Optimizely to transfer; 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 acknowledges that Optimizely (as Processor) has no contractual (or other) relationship with those 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 sole responsibility for such compliance.

2.6 Customer shall ensure on an ongoing basis that the Processing of such Personal Data by such third parties shall comply with applicable Data Protection Laws and shall inform Optimizely immediately should it become aware that any transfer of such Personal Data by Optimizely no longer complies with Data Protection Laws, in which case Optimizely shall be entitled to discontinue such transfers and Customer shall promptly take such measures as are required to remedy such non-compliance.

2.7 *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**.

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 Personal Data are informed of the confidential nature of the Personal 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 Personal 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 Personal 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 after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored, or otherwise Processed by Optimizely or its Sub-processors of which Optimizely becomes aware (“*Customer Data Incident*”).

3.3.2 Identify, Remediate and Inform. Upon becoming aware of a Customer Data Incident, Optimizely shall promptly: (i) make all reasonable efforts to identify the cause of such Customer Data Incident, (ii) take those steps as Optimizely deems necessary and reasonable in order to remediate the cause of such a Customer Data 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 incident on any Data Subjects in relation to such Personal Data and/or on Customer, and (v) otherwise co-operate with Customer in investigating and dealing with such incident and its consequences. The obligations herein shall not apply to incidents that are caused by Customer or Customer’s Users.

3.4 *Deletion and/or Return of Customer Data*

3.4.1 Deletion and/or Return. Optimizely shall not acquire any rights in such Personal Data and, on Customer’s request or thirty (30) days after the termination or expiration of the Agreement, will to the extent allowed by applicable law, permanently destroy all copies of any such Personal Data in its possession (in any form or format whatsoever) using industry standard destruction methods. 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 5.

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 specify whether Personal Data Processing is permitted, 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 expressly permitted – and then only Process the Personal Data as expressly permitted in the Service Description.

5.2 Sensitive Information. Notwithstanding anything to the contrary in any Service Description, the Software Services are not intended to Process Sensitive Information. Customer is solely responsible for determining whether using the Software Service to Process Sensitive Information complies with Data Protection Laws. If Customer processes Sensitive Information in its Use of the Software Service, Customer is acknowledging that Optimizely's TOMs are sufficient and satisfactory for its purposes in relation to its 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 The Audit will be subject to the requirements set out above in Section 7.1;

7.3.2 Customer may not Audit Optimizely more than once annually (unless otherwise required by government regulator or Supervisory Authority or triggered by a security breach) 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 Customer will submit a detailed audit plan (“**Audit Plan**”) at least 10 business days in advance and be mutually agreed by the Parties at least 5 business days in advance of the scheduled Audit date – any delay may require a re-scheduling of the Audit;

7.3.4 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 if Customer's current total yearly spend with Optimizely is less than \$30,000 US 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 Personal 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 Personal 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/s/participant-search/participant-detail?id=a2zt000000PD4sAAG&status=Active>. 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 *SCCs.* The Parties agree that the terms of the SCCs, as set out in **Exhibit 2** and **Exhibit 2A** of this DPA, are hereby incorporated and apply to any 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.

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

10.1 *Search.* Where Customer's Personal 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 Personal Data affected thereby is in Customer's sole property and area of responsibility, that Personal Data is at Controller's sole disposition, and that Controller is the responsible body in the sense of Data Protection Laws.

10.2 *DPA Updates.* Where updates to this DPA (including the TOMs) 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. Such amendment may include, for example, the introduction of replacement or additional SCCs in the form of any standard data protection clauses adopted under GDPR Art 46 from time to time.

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 regulations of this DPA shall not be affected.

10.5 *Additional GDPR Specific Provisions:*

10.5.1 GDPR. Optimizely will Process Personal Data in accordance with the GDPR requirements directly applicable to Optimizely’s provision of its Software Service.

10.5.2 Data Protection Transfer Impact Assessment. Upon Customer’s reasonable request, Optimizely shall provide Customer with commercially reasonable assistance to assist Customer in its obligation under applicable Data Protection Laws to carry out a data protection transfer impact assessment related to Customer’s use of the Software Service – (“DPTIA”). 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 inwith respect to its assistance to Customer in its DPTIA to the extent required under applicable Data Protection Laws.

EXHIBITS follow:

- Exhibit 1: [Details of the Processing](#)
- Exhibit 2: [Standard Contractual Clauses \(Module Two\)](#)
- Exhibit 2A: [Standard Contractual Clauses \(Module Three\)](#)
- Exhibit 3: [UK Addendum to the EU Commission Standard Contractual Clauses](#)
- Exhibit 4: [US Data Protection Law Addendum](#)