

INTRODUCTION

The Data Processing Agreement ("**DPA**") forms part of the Agreement between Company 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 Company processes Personal Data for which such Affiliates 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 "**Company**" means the Optimizely Group company as set out in the Order Form

1.2 "**Optimizely Group**" means Company and its Affiliates.

1.3 "**Optimizely BCR**" means Optimizely Group's binding corporate rules for Data Processing, the most current version of which is available on Company's website (located at: <http://www.optimizely.com/trust-center/>, as updated from time to time) which govern transfers of Personal Data to Third Countries to, and between, Company Group members, and to third-party Sub-processors.

1.4 "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

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**.

NOTE: Where the relevant Data Protection Laws are the laws and regulations of the United Kingdom, references to "**Standard Contractual Clauses**" or "**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 Company or a member of the Company Group.

1.14 "**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR or is a regulatory authority under any other Data Protection Laws.

1.15 "**Third Country**" means any country, organization or territory not acknowledged by the European Union based on Article 45 of GDPR as a safe country with an adequate level of data protection.

2. PROCESSING OF PERSONAL DATA

2.1 *Roles of the Parties.* As between the parties, Customer is the Controller and Company 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**.

2.2 *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. Notwithstanding anything to the contrary in any Service Description, no Sensitive Information Processing is permitted. For clarity and certainty, Customer is not permitted to upload any Sensitive Information into the Software Service.

2.2.1 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.

2.2.2 Customer shall ensure it complies with the restrictions set out above, except to the extent that Company and Customer may have otherwise agreed in writing (signed by the Company).

2.3 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 2.1 or because required supplementary measures were not implemented as a result of a failure by Customer to notify Company of the requirement for them.

2.4 *Company's Processing.* Personal Data is Customer Confidential Information, and the confidential obligations of the Agreement apply to that Personal Data. Company 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. Company shall be entitled to Process Personal Data in Third Countries outside the EU/EEA, including, in particular, (but without limitation) Vietnam, Australia, the United States, and the United Kingdom for support purposes. Upon request, Company shall update Customer with updates to its countries where Software Service support are located.

2.5 *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

2.5.1 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;

2.5.2 ensuring that any transfers of Personal Data to third parties (other than Company 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 Company pursuant to Customer's instructions, comply with Data Protection Laws.

2.5.3 determining the Personal Data it transfers or instructs Company to transfer,

2.5.4 assessing which Data Protection Laws apply to such transfer,

2.5.5 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).

2.6 Customer acknowledges that Company (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.

2.7 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 Company immediately should it become aware that any transfer of such Personal Data by Company no longer complies with Data Protection Laws, in which case Company shall be entitled to discontinue such transfers and Customer shall promptly take such measures as are required to remedy such non-compliance.

2.8 *Details of the Processing.* The subject-matter of Processing of Personal Data by Company 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 *Company Resources, Personnel, and Employees*

3.1.1 Confidentiality. Company 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. Company shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

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

3.1.3 Assistance. Company 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. Company shall ensure that Company'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 Company Group has appointed a data protection officer. The appointed person may be reached at dpo@optimizely.com.

3.2 *Security*

3.2.1 Controls for the Protection of Customer Data. Company shall maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of the Customer Data ("**TOMs**"), as made currently available (as updated from time to time at: <https://www.optimizely.com/trust-center/privacy/toms/>). The company maintains a formal program to maintain the ToMs and respond to emerging risks, changes in applicable legal requirements, technical and organizational changes.

3.2.2 Company regularly monitors the effectiveness and compliance with the TOMs. The TOMs are subject to update from time to time for purposes of continuous improvement. Security as described in the TOMs will not materially decrease during a Subscription term.

3.2.3 Controls and Auditing. Company maintains technical and organizational controls to protect the confidentiality, availability and integrity of customer data and provided services. Company routinely audits those controls 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, Company shall make available to Customer (or Customer's independent, third-party auditor) documentation and evidence of the effectiveness of the controls, as applicable, subject to the safeguarding of Company's legitimate interests and to the extent commercially feasible. Notwithstanding the rest of this Section 3.2.3, Customer acknowledges that Company may at its own discretion refuse 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 Company 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, unauthorised disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Company or its Sub-processors of which Company becomes aware ("**Customer Data Incident**").

3.3.2 Upon becoming aware of a Customer Data Incident, Company shall promptly: **(i)** make all reasonable efforts to identify the cause of such Customer Data Incident, **(ii)** take those steps as Company deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Company'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 Company shall not acquire any rights in such Personal Data and, on Customer's request or 30 days after the termination or expiration of this 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 a readable format. Cost to reformat returned data to Customer specifications is borne by the Customer.

4. OBLIGATIONS OF CONTROLLER

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

4.2 Customer shall inform Company without undue delay and comprehensively about any errors or irregularities related to the Processing of Personal Data detected.

4.3 Customer shall inform Company without undue delay and comprehensively if it identifies any Personal Data being Processed in its use of the Software Services that contravenes Section 2.1 and, where required by Company to do so, shall promptly take such steps as Company may require to bring its use of the Software Services into conformance with Section 2.1.

4.4 Company provides the base Software Services, which Customer is then responsible for implementing (which may include, but is not limited to, modifying, customizing, editing and configuring the base Software Services) ("**Implementation**"). Company will not have any responsibility or liability that may result from Customer's implementation of the Software Services.

5. DATA SUBJECT RIGHTS

5.1 Company shall, to the extent legally permitted, promptly notify Customer if Company receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("**right to be forgotten**"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**"). Taking into account the nature of the Processing, Company shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. Customer acknowledges that in most cases, Customer should have the ability to address a Data Subject Request pertaining to the use of the Software Services independently. If however, Customer, in its use of the Software Services, is not able to address a Data Subject Request independently, Company shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Company is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Company's provision of such additional service assistance.

5.2 In order for Company to use commercially reasonable efforts to assist Customer in responding to Data Subject Requests, as per Section 5.1 of this DPA, Company may request a data map from Customer of Customer's solution built on the Software Services. Customer must ensure that it does not send duplicative or otherwise incomplete Data Subject Requests, as assessed under the Data Protection Laws, to the Company.

5.3 Notwithstanding Sections 5.1 and 5.2, the Company shall only provide assistance in relation to Data Subject Requests where the Personal Data in question is Processed by Company, and therefore shall not extend to Personal Data Processed outside of the Software Services over which the Customer is responsible.

6. DPA AUDITS

6.1 Customer may, prior to the commencement of Processing, subject to the confidentiality obligations under the Agreement, audit the TOMs taken by Company as it relates to Processing within Customer's Software Services, and shall document the resulting findings. Customer may also appoint an independent third-party auditor (that is not a competitor of Company) ("**Auditor**") to conduct such audit.

6.2 For such purpose, Customer may,

6.2.1 obtain information from Company (or Company Sub-processor),

6.2.2 request Company (or Company Sub-processor) to submit to Customer an existing attestation or certificate by an independent professional expert, or

6.2.3 upon reasonable and timely advance agreement, during regular business hours and without interrupting Company's business operations, and at Customer's sole cost, conduct an on-site inspection of Company's business operations or have the same conducted by an Auditor

6.3 Company shall, upon Customer's written request and within a reasonable period of time, provide Customer with all reasonable information necessary for such audit, except to the extent such disclosure of information would violate Company contracts and/or security and other related policies and procedures. Customer shall promptly notify Company with information regarding any non-compliance discovered during the course of an audit.

6.4 Audits conducted under this Section 6:

6.4.1 Will be performed after Customer review of existing industry-standard third-party audit attestations.

6.4.2 will be performed no more than once per calendar year (unless otherwise required by government regulator or Supervisory Authority or triggered by a security breach);

6.4.3 will be scheduled at least sixty (60) days in advance with Customer submitting a detailed proposed audit plan to Company at least two weeks in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit with Company; and

6.4.4 may be subject to an added cost where the cost of the audit exceeds 2% of the total annual contract commitment under the Master Services Agreement.

7. SUB-PROCESSORS

7.1 Appointment of Sub-processors. Customer acknowledges and agrees that **(a)** Company's Affiliates may be retained as Sub-processors; and **(b)** Company and Company's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Software Services. Company or a Company 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 Company shall be entitled to leverage Standard Contractual Clauses for processor to processor transfers. Controller hereby authorizes Company to conclude such Standard Contractual Clauses with the relevant Sub-contractors domiciled in Third Countries.

7.2 List of Current Sub-processors and Notification of New Sub-processors. Company shall make available to Customer the current list of Sub-**Exhibit 2.** Customer may find then current on Company's Trust Center Resources webpage (also accessible via <https://www.optimizely.com/trust-center/privacy/sub-processors/>). Company shall provide Notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process the Customer's Personal Data. Such Notification is provided at <https://status.optimizely.com/> and functionality for subscription is available at web page.

7.3 Objection Right for New Sub-processors. Customer may object to Company's use of a new Sub-processor by notifying Company promptly in writing within thirty (30) days after receipt of Company'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, Company 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 Company 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 Company without the use of the objected-to new Sub-processor by providing written notice to Company. Company will refund any pre-paid, unused fees following the effective date of termination with respect to such terminated Software Services.

7.4 Liability. Company shall be liable for the acts and omissions of its Sub-processors to the same extent Company 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.

8. INTERNATIONAL TRANSFERS

8.1 Without prejudice to Section 8.2 where it applies, the SCCs apply only to Personal Data that is transferred to a Third Country, either directly or via onward transfer, that is not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to binding corporate rules for processors.

8.2 Where the relevant Data Protection Laws are the laws and regulations of the United Kingdom, SCCs approved under UK GDPR Art 46 may apply to Personal Data that is transferred from the United Kingdom to a Third Country that is not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to binding corporate rules for processors.

8.3 The Company entity listed in the Standard Contractual Clauses in **Exhibit 2** (or any new version of the SCCs that replace them) is a party to the SCCs. Any other Company entities not named are not a party to this DPA or the Standard Contractual Clauses. Where Company is a different legal entity than Optimizely Inc. or Episerver, Inc., Company is carrying out the obligations of the data importer as set out in SCCs on behalf of Optimizely Inc. or Episerver, Inc.

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

9.1 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, Company shall inform Customer without undue delay unless legally prohibited. Company 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.

9.2 With respect to updates and changes to this DPA, Company shall be entitled to make amendments or changes to the terms of this DPA upon giving Customer at least ninety (90) days' prior notice where such amendments or changes are required in its reasonable opinion as a result of any changes to the requirements of Data Protection Laws. Such amendments and changes may include the introduction of replacement or additional SCCs to those contained in Appendix 1 in the form of any standard data protection clauses adopted under GDPR Art 46 from time to time.

9.3 In the event that Software Services are 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 Optimizely BCR; and **(2)** the Standard Contractual Clauses. The transfer mechanisms referenced in this Section 8.3 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 Section 2 of this DPA.

9.4 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.

9.5 The section “*Limitations of Liability*” in the Agreement shall apply to this DPA

9.6 Additional European Specific Provisions:

9.6.1 GDPR. Company will Process Personal Data in accordance with the GDPR requirements directly applicable to Company's provision of its Software Services.

9.6.2 Data Protection Transfer Impact Assessment. upon Customer’s request, Company shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer’s obligation under the GDPR to carry out a data protection transfer impact assessment related to Customer’s use of the Software Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Company. Company shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 9.6.2 of this DPA, to the extent required under the GDPR.

EXHIBITS follow

- Exhibit 1: [Details of the Processing](#)
- Exhibit 2: [Standard Contractual Clauses](#)