Data Processing Agreement (DPA)

Appendix 3 to MSA (GDPR, Standard Contractual Clauses (2021), Company Processor Binding Corporate Rules)

Updated July 17th, 2021

INTRODUCTION

The Data Processing Agreement ("**DPA**") forms part of the Master Services Agreement, including all Orders, appendices and references, or other written or electronic agreement between Company and Customer for the purchase of online services from Company (identified either as "**Software Services**" or otherwise in the applicable agreement, and hereinafter defined as "**Software Services**") (the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data.

By signing this Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Company processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "**Customer**" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement, end-user services agreement ("**EUSA**") and service level agreement ("**SLA**").

In the course of providing the Software Services to Customer pursuant to the Agreement, Company may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA and Exhibits 1 (including the Appendix), 2 and 3.
2. If this DPA is attached to an Agreement or Order which is signed and executed, the DPA will become legally binding between the Parties as part of the Agreement or Order.
3. If this DPA was not attached to an Agreement or Order, then this DPA has been pre-signed on behalf of Company and Customer must follow Step 4 below. The Standard Contractual Clauses in Exhibit 1 have been pre-signed by Company as the data importer.
4. To complete this DPA when not attached to an Agreement or Order, Customer must:
    a. Complete the information in the signature box and sign on Page 7.
    b. Take note that different Sub-processors apply to different Services on Page 16.
    c. Send the completed and signed DPA to Company by email or webform, indicating the Customer's Account Name (as set out on the applicable Company Agreement, Order or invoice), which will be addressed to dpa@optimizely.com. Upon receipt of the validly completed DPA by Company at this email address or webform, this DPA will become legally binding.

HOW THIS DPA APPLIES

If Customer entering into this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Company entity that is party to the Agreement is party to this DPA.

If Customer's Affiliate entering into this DPA has executed an Order with Company or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order and applicable renewal Orders, and the Company entity that is party to such Order is party to this DPA.

If the Customer entity signing the DPA is not a party to an Order nor a Master Services Agreement directly with Company but is instead a customer indirectly via an authorized reseller of Company services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

This DPA shall not replace any additional terms relating to Processing of Customer Data contained in any Amendment(s) to Customer's Agreement, however shall replace any existing standard data processing agreement between the Parties.

If an entity signing this DPA is neither a party to an Agreement nor an Order, this DPA is not valid and is not legally binding. Such entity should request that a Customer entity who is a party to the Agreement executes this DPA on their behalf.

**Note: If Customer is using Episerver Managed Services (formerly Everweb or Ektron Holding), this DPA is not valid and is not legally binding unless written confirmation from Company has been received stating that the minimum GDPR technical and organizational measures on Customer's environment have been met.*

Terms of the DPA

1. Definitions

1.1. **“Affiliate”** means any entity that Controls, is controlled by, or is under common control of either Party to this Agreement. The term “**Control**” shall mean the power or authority to direct influence over the operations of an entity, as indicated by the holding of a majority share of the voting stock of such entity, and in relation to the Company means the Episerver entity that is a party to this Agreement and/or signs an Order or other documentation as part of the Agreement, including Optimizely Inc., a company incorporated in Delaware, USA, Episerver Inc., a company incorporated in Delaware, USA, Episerver AB, a company registered in Sweden, Episerver UK Ltd., a company registered in England and Wales, Episerver GmbH, a company registered in Berlin, Germany and Insite Software Solutions Inc., a company incorporated in Delaware.

1.2. **“Authorized Affiliate”** means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Software Services pursuant to the Agreement between Customer and Company as specified on the applicable Order Form or MSA.

1.3. **"Company"** means the entity which is a party to this DPA which is a member of the Company Group.

1.4. **“Company Group”** means Company and its Affiliates engaged in the Processing of Personal Data including Optimizely, Inc., a corporation incorporated in Delaware, USA, Episerver Inc., a company incorporated in Delaware, USA, Episerver AB, a company registered in Sweden, Episerver UK Ltd., a company registered in England and Wales, Episerver GmbH, a company registered in Berlin, Germany, Episerver Research and Development Company Limited, a company registered in Vietnam, Episerver Pty Ltd, a company incorporated in New South Wales, Australia, Insite Software Solutions Inc., a corporation incorporated in Delaware, USA, Idio Inc., a company incorporated in Delaware, USA and Zaius Inc., a corporation incorporated in Delaware, USA.

1.5. **“Company BCR”** means Company Group’s processor binding corporate rules for the Processing of Personal Data, the most current version of which is available on Company’s website, currently located at: http://www.optimizely.com/trust-center/ which govern transfers of Personal Data to third countries to and between members of the Company Group, and to third-party Sub-processors. The scope of application of the Company BCR is set out in Section 8.3 of this DPA.

1.6. **“Controller”** means the entity which determines the purposes and means of the Processing of Personal Data.

1.7. **“Customer Data”** means what is defined in the Agreement as “**Customer Data**” or “**Your Data**.”

1.8. **“Data Privacy, Protection, Security and Architecture Documentation”** or **“DPPSAD”** means the documentation available to Customer regarding data privacy, protection, security and architecture documentation applicable to the Software Services purchased by Customer, as updated from time to time, and accessible in the Standard Contractual Clauses Appendix 1 and 2, or via Company’s Trust Center, https://www.optimizely.com/trust-center/, and Optimizely World https://world.optimizely.com/, or as otherwise made reasonably available by Company.

1.9. **“Data Protection Laws and Regulations”** means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including (but not limited to) laws and regulations of the European Union (“**EU**”), the European Economic Area (“**EEA**”) and their member states, Switzerland and the United Kingdom.

1.10. **“Data Subject”** means the identified or identifiable person to whom Personal Data relates.

1.11. **“GDPR”** means (i) the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation) and (ii) in the context of processing of Personal Data where the applicable Data Protection Laws and Regulations regulating that processing are those of the United Kingdom, the UK GDPR (as defined in the Data Protection Act 2018).

1.12. **"Geofencing"** has the meaning given to that term in Exhibit 3 (Supplementary Measures).

1.13. **“Personal Data”** means any information (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 applicable Data Protection Laws and Regulations, where for each (i) and (ii), such data is Customer Data.

1.14. **“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.

1.15. **“Processor”** means the entity which Processes Personal Data on behalf of the Controller.

1.16. **“Standard Contractual Clauses”** or **"SCCs"** means the agreement executed by and between Customer and Company and attached hereto as Exhibit 1 pursuant to the European Commission’s decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection and any replacement agreement entered into between Customer and Company from time to time pursuant to Exhibit 3 (Supplementary Measures). Where the relevant Data Protection Laws and Regulations 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.

1.17. **“Sub-processor”** means any Processor engaged by Company or a member of the Company Group.

1.18. **“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 and Regulations.

2. Processing of Personal Data

2.1. **Software Services Restrictions**. The Parties agree that the Software Services provided by Company are as described in the service descriptions that are available at https://world.optimizely.com/services/descriptions/. These service descriptions specify whether a particular Software Service permits Customer to process Personal Data within it or not. Where a particular Software Service description provides that the Software Service does not permit Personal Data to be Processed within it (or where it permits Personal Data to be processed within it, the description provides that the permitted Personal Data and/or Processing concerned is restricted, including (but not limited to) by the requirement for Geofencing) then Customer shall:

2.1.1. (where the Software Service description provides that the Processing of Personal Data is not permitted), not Process Personal Data within the relevant Software Service; and/or

2.1.2. (where the Software Service description provides that the Processing of Personal Data is restricted), not Process Personal Data within the relevant Software Service other than in compliance with the relevant restriction;

Customer shall ensure the limitations and restrictions for processing as stated above are met in each case, other than to the extent that Company may have otherwise agreed in writing from time to time. This Section 2.1 takes effect precedence over any other term in this DPA to the contrary and references in the remainder of this Agreement to Personal Data and Processing shall be construed accordingly.

2.2. **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Company is the Processor and that Company or members of the Company Group will engage Sub-processors pursuant to the requirements set forth in Annex III of the Appendix to Exhibit 1 ("**Sub-processors**") below.

2.3. **Company's Processing of Personal Data.** Company shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order(s); (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 theAgreement.

2.4. **Customer's Processing of Personal Data.** Customer shall, in its use of the Software Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. 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. identifying any databases containing Personal Data to which Geofencing restrictions are to be applied in order to comply with Data Protection Laws and Regulations and the notice requirement for such restrictions pursuant to Exhibit 3 (Supplementary Measures); and

2.4.3. 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 and Regulations, including (without limitation) ensuring compliance with the requirements of GDPR Arts 44-49 where they apply. As Controller, Customer agrees that it is solely responsible for (i) determining the Personal Data it transfers or instructs Company to transfer, (ii) assessing which Data Protection Laws and Regulations apply to such transfer, and (iii) 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). Customer agrees 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. As Controller, 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 Regulations 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 and Regulations, 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. Without prejudice to the foregoing provisions of this Section 2.4.3, 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 and Regulations.

2.5. **Details of the Processing.** The subject-matter of Processing of Personal Data by Company is the performance of the Services pursuant to the Agreement. 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 2 (Details of the Processing, Categories of Data and Data Subjects) to this DPA.

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. 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.

3.1.4. 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.

3.1.5. Territory. Customer confirms that, for the purposes of this DPA, subject only to

3.1.5.1. any Geofencing restrictions notified in accordance with Exhibit 3 (Supplementary Measures), and/or

3.1.5.2. any specific additional measures that have been agreed by Customer and Company pursuant to Exhibit 3 (Supplementary Measures);

Company shall be entitled to Process Personal Data under this DPA in third countries outside the EU/EEA, including, in particular, Vietnam, Australia, the United States, and the United Kingdom for support purposes only.

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 Customer Data, as set forth in the DPPSAD. This includes, but is not limited to –

3.2.1.1. the prevention, where Processor reasonably can, of unauthorized persons from gaining access to Software Services processing Personal Data (physical access control),

3.2.1.2. the prevention, where Processor reasonably can, of Software Services processing Personal Data from being used without authorization (logical access control),

3.2.1.3. ensuring, where Processor reasonably can, that persons entitled to use Software Services processing Personal Data gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights and Controller's instructions, and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control),

3.2.1.4. ensuring, where Processor reasonably can, that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),

3.2.1.5. ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems (entry control),

3.2.1.6. ensuring that where Processor is Processing Personal Data, that they are done solely in accordance with the Customer's instructions (control of instructions),

3.2.1.7. ensuring, where Processor reasonably can, that Personal Data are protected against accidental destruction or loss (availability control),

3.2.1.8. ensuring, where Processor reasonably can, that Personal Data collected for different purposes can be processed separately, based on Customer's instructions (separation control), use of, where applicable and reasonably practicably possible, industry standard encryption and/or pseudonymization.

3.2.2. Company regularly monitors compliance with these measures in the aforementioned Section 3.2.1. Company will not materially decrease the overall security of the Software Services during a Subscription term.

3.2.3. Third-Party Certifications and Audits. Company has obtained the third-party certifications and audits set forth in the DPPSAD. 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 that is not a competitor of Company (or Customer's independent, third-party auditor that is not a competitor of Company) a copy of DPPSAD's then most recent third-party audits or certifications, as applicable, subject to the safeguarding of Company's legitimate interests and to the extent commercially feasible.

3.3. **Customer Data Incident Management and Notification**

3.3.1. Company maintains security incident management policies and procedures specified in the DPPSAD and 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 toincidents 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 demand, will either return to the Customer or destroy and/or, to the extent allowed by applicable law, permanently delete from its information systems (at the option of Controller) all copies of any such Personal Data in its possession (in any form or format whatsoever) in accordance with the procedures and timeframes specified in the DPPSAD.

4. Obligations of Controller

4.1. Customer and Company shall be separately responsible for conforming with such statutory data protection regulations, including but not limited to Data Protection Laws and Regulations as are applicable to them.

4.2. Customer shall inform Company without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data detected during a verification of the results of such Processing.

4.3. Customer shall inform Company without undue delay and comprehensively if:

4.3.1. 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; and

4.3.2. special categories of Personal Data in accordance with GDPR Article 9 are to be Processed or if there are peculiarities in the assessment for other reasons, in particular if there is an increased probability of occurrence or seriousness of risks in relation to the Data Subject's rights. Further, Customer shall take note of terms and conditions related to Sensitive Information within the Agreement and must provide Company a data map prior to the Processing of the aforementioned data.

4.4. Customer shall comply with its obligations as controller in relation to its Processing of the Personal Data under Data Protection Laws and Regulations, including (without limitation):

4.4.1. general data protection principles (GDPR Article 1-5) and fulfilment of Data Subject Request (GDPR Article 15-22),

4.4.2. fulfilling the duties to affirmative consent (GDPR Article 4(11), 7), inform and transparency (GDPR Article 12-14) and record keeping (GDPR Article 30).

4.5. Customer shall, upon termination or expiration of the Agreement and by way of issuing a written instruction, stipulate, within a period of time set by Company, the reasonable measures to return data carrier media or to delete stored data.

4.6. To the extent allowed by applicable law, any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by Customer

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 and Regulations. In addition, to the extent Customer, in its use of the Software Services, does not have the ability to address a Data Subject Request, 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 and Regulations. 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 incompetent Data Subject Requests, as assessed under the Data Protection Laws and Regulations, 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 technical and organisational measures 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 to conduct such audit. Such audit guidelines and principles are further detailed in the Agreement between the parties.

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 a qualified third party which shall not be a competitor of Company.

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 no more than once per calendar year (unless otherwise required by government regulator or Supervisory Authority);

6.4.2. will be scheduled at least sixty (60) days in advance of taking place with Customer submitting a detailed proposed audit plan to at least two weeks in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit with Optimizely reviewing on approving the proposed audit plan; and

6.4.3. 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 to 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 enter to Standard Contractual Clauses being such clauses relevant 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-processors for the Services identified in Annex III of the Appendix to Exhibit 1. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location (“**Infrastructure and Sub-processor Documentation**”). 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 Personal Data in connection with the provision of the applicable Services. 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. Duties to Inform, Mandatory Written Form, Choice of Law, Additional Terms

8.1. 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. 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 and Regulations.

8.2. 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 and Regulations. Such amendments and changes shall 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 and any other changes of a type contemplated in Exhibit 3 (Supplementary Measures). Subject to the foregoing provisions of this Section, the terms that apply in the 'Amendment; No Waiver' Section 10 in the EUSA shall apply.

8.3. 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 Company Processor BCR, and. (2) the Standard Contractual Clauses.

8.4. 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.

8.5. The SCCs will apply to the processing of Personal Data by Processor under the Agreement. Upon the incorporation of this DPA into the Agreement, the parties indicated in Section 9 below (Parties to this DPA) are agreeing to the SCCs and all appendixes attached thereto as updated in accordance with Section 8.2 from time to time.

8.6. Without prejudice to Section 8.7 where it applies, the SCCs apply only to Personal Data that is transferred from the European Economic Area (EEA) to outside the EEA, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR), and (ii) 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.

8.7. Where the relevant Data Protection Laws and Regulations 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, either directly or via onward transfer, to any country or recipient: (i) not recognized by regulations made under the Data Protection Act 2018 as providing an adequate level of protection for personal data (as described in the GDPR), and (ii) 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.

8.8. **Additional European Specific Provisions:**

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

8.8.2. Data Protection 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 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 8.8.2 of this DPA, to the extent required under the GDPR.

8.8.3. Transfer mechanisms for data transfers. Subject to the additional terms in Annex II of Exhibit 1, Company makes available the transfer mechanisms listed below which shall apply, in the order of precedence as set out in Section 8.3, to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations:

8.8.3.1. The Company BCRs apply to the Software Services listed in the Agreement and/or Order(s) and subject to this DPA;

8.8.3.2. The SCCs set forth in Exhibit 1 to this DPA apply to the Software Services listed in the Agreement and/or Order(s) which are required for Company Software Services support purposes only.

The transfer mechanisms referenced in this Section 8.8.3 are made available to apply to Processing 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:

8.8.3.3. not Process Personal Data in contravention of any Software Service prohibitions or limitations on the Processing of Personal Data referenced in Section 2.1; and

8.8.3.4. notify Company of any Geofencing restrictions required in terms of Exhibit 3 (Supplementary Measures) so that appropriate Geofencing restrictions can be applied; and accordingly, Customer agrees that, as Controller, it is solely responsible for compliance with the requirements of Data Protection Laws and Regulations with regard to any Processing of Personal Data under this DPA which involves transfers of Personal Data which occur in contravention of Section 8.8.3.3 or because required Geofencing restrictions were not implemented as a result of a failure by Customer to notify Company of the requirement for them under Section 8.8.3.4. The provisions of this Section 8.8.3 are also without prejudice to the provisions of Section 2.4.3 where they apply.

9. Parties to the DPA

9.1. The Section “HOW THIS DPA APPLIES” specifies which Company entity is party to this DPA. In addition, The Company entity listed in the Standard Contractual Clauses in Exhibit 1 (or any SCCs that replace them as contemplated under Exhibit 3 (Supplementary Measures) 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. Further the section “Limitations of Liability” in the Agreement shall apply to this DPA.

9.2. Authorized Affiliates. Parties acknowledge and agree that, by executing the Agreement, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Company and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 9 and Section 10. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Software Services and Customer Data by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

9.2.1. Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Company under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.2.2. Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Company, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.2.2.1. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Company directly by itself, the parties agree that (i) solely Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 9.2.4. below).

9.2.2.2. Parties agree that Customer that is the contracting party to the Agreement shall, when carrying out an on- site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Company and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. Legal Effect

This DPA shall only become legally binding between Customer and Company when the formalities steps set out in the Section “HOW TO EXECUTE THIS DPA” above have been fully completed.

Parties' authorized signatories have duly executed this Agreement:

Company	**Customer:**
Signature: ______________________	Signature: ______________________
Print name: ______________________	Print name: ______________________
Title: ______________________	Title: ______________________
Place and Date: ______________________	Place and Date: ______________________

EXHIBIT 1

Standard Contractual Clauses (Controllers to Processors)

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer").

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1), and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract, and/or to add other clauses or additional safeguards provided that they do not contradict, directly or indirectly these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and / or data importer, with the following exceptions:

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

ii. Clause 8.1(b), 8.9(a), (c), (d) and (e);

iii. Clause 9(a), (c), (d) and (e)

iv. Clause 12(a), (d) and (f);

v. Clause 13;

vi. Clause 15.1(c), (d) and (e);

vii. Clause 16(e); and

viii. Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 *Instructions*

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions

8.2 *Purpose limitation*

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 *Transparency*

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 *Accuracy*

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 *Duration of processing and erasure or return of data*

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 *Security of processing*

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 *Sensitive data*

Where the transfer involves 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 (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 *Onward transfers*

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii. (the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 *Documentation and compliance*

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.8 The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  ii. refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws affecting compliance with the Clauses.

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 *Notification*

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii. (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 *Review of legality and data minimisation*

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISION

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii. the data importer is in substantial or persistent breach of these Clauses; or

iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Sweden.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of Sweden.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX to the Standard Contractual Clauses

This Appendix forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

ANNEX I.

A. LIST OF PARTIES

Data exporter. The data exporter is the **Customer**, as defined in the Agreement (such as Master Services Agreement "MSA" or Master Managed Services Agreement "MMSA") and/or Order(s).

Data importer. The data importer is **Company**, as defined in the Agreement (such as Master Services Agreement ("MSA") or Master Managed Services Agreement ("MMSA") and/or Order(s).

B. DESCRIPTION OF TRANSFER

Categories of data subjects

Content/Commerce Clouds, Personalization: The personal data transferred concern the Customer's end users including employees, contractors and the personnel of customers, suppliers, collaborators, and subcontractors. Data Subjects also includes individuals attempting to communicate with or transfer personal information to Customer's end users.

Experimentation/Full Stack: The personal data transferred concern the Customer's end users and visitors to the Customer's website and apps.

Optimizely Data Platform: The personal data transferred concern the Customer's end users including employees, contractors and the personnel of customers, suppliers, collaborators, and subcontractors. Data Subjects also includes individuals attempting to communicate with or transfer personal information to Customer's end users.

Categories of personal data transferred

Content/Commerce Clouds, Personalization: The personal data transferred concern personal data, entity data, navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by end users via the Software Service(s) and/or Managed Service(s).

Experimentation/Full Stack: The personal data transferred concern:

- Website and app visitors: IP addresses, random unique identifiers such as cookie IDs or similar identifiers, and experiment and event data associated with these identifiers (such as device type, variation and experiment IDs, browser and OS version and the elements of the site being tested) based on Customer's use and configuration of the Optimizely Service. Customer may take advantage of features of the Optimizely Service such as IP address anonymization to minimize collection of such data and must comply with any prohibitions in the Governing Agreement relating to restrictions on collection and use of Personal Data.
- Customer end users: Names, email addresses, passwords, contact details, and similar Personal Data provided by Customer End Users when creating an Optimizely account.

Optimizely Data Platform: The personal data and non-personal data transferred involve the following:

- Website and app visitors: IP addresses, random unique identifiers such as cookie IDs or similar identifiers, event data associated with these identifiers (such as device type, browser and OS version and the elements of the site being tested) based on Customer's use and configuration of the Optimizely Service. Customer may take advantage of features to minimize collection of such data and must comply with any prohibitions in the Governing Agreement relating to restrictions on collection and use of Personal Data.
- Customer end users: Names, email addresses, passwords, contact details, and similar Personal Data provided by Customer End Users when creating an Optimizely account.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

All Software Services: The parties do not anticipate the transfer of special categories of data.

Frequency of processing

All Software Services: Data will be transferred on a continuous basis.

Nature of the processing

All Software Services: Customer determines the types of data they submit to Company to process on their behalf in the course of using Company's services. The Company has no direct relationship with the individuals whose information it receives from its customers or their business partners. The Company does not control such information, does not select or determine the specific types of data that it processes, and does not determine the purpose for which it is processed.

In other instances, Company may collect Personal Data when performing expert services at its customers' request, to provide customer support, in general support of its customer relationships, which may include but are not limited to marketing activities, fulfilling product orders, to improve product offerings, customer surveys, questionnaires, responses to comments, etc., to download software and/or gain access to and/or enable certain products or services, for internal business processes, such as financial processing, responding to informational requests, and to comply with applicable laws.

Experimentation/Full Stack: In addition to the above, Company will provide the feature flagging, personalization, analytics and/or other Software Services ordered by Customer according to the Instructions. Company will also provide customer end users with reporting, communications and other features offered by the Company.

Purposes of the data transfer and further processing

All Software Services: Personal data may be processed for the following purposes: (a) to provide the Software Service (which may include the detection, prevention and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfill the obligations under the Company End-User Services Agreement and Service Level Agreement or the Company Managed Services General Terms and Conditions and Service Level Agreement (for Managed Services Customers). The Customer instructs Company to process personal data in countries in which Company or its subprocessors maintain facilities as necessary for it to provide the Software Service(s). [Note: Language to be reviewed and updated.]

Term of Data Processing

All Software Services: Data processing will be for the term specified in the Company End-User Services Agreement or the Company Managed Services General Terms and Conditions (for Managed Services Customers). For the term of the End-User Services Agreement or the Company Managed Services General Terms and Conditions (for Managed Services Customers), and for a reasonable period of time after the expiry or termination of the Agreement, the Data Importer will provide Customer with access to, and the ability to export, Customer's personal data processed pursuant to the Agreement.

Data Deletion

All Software Services: For the term of the Agreement, Company will provide Customer with the ability to delete data as detailed in the Agreement.

Access to Data

All Software Services: For the term of the Agreement, Company will provide Customer with the ability to correct, block, export and delete Customer's personal data from the Software Service(s) and/or Managed Service(s) in accordance with the Agreement.

Subprocessors

All Software Services: The Company may engage subprocessors to provide parts of the Software Service and/or Managed Service(s). The Company will ensure subprocessors only access and use Customer's personal data to provide Company's products and services and not for any other purpose. Details found in Annex III.

C. DESCRIPTION OF TRANSFER

Swedish Authority for Privacy Protection (Datainspektionen)

ANNEX II. TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The details of the technical and organizational measures applicable to the Software Services being provided by Company to Customer can be found at https://www.optimizely.com/trust-center/privacy/toms/.

ANNEX III. LIST OF SUBPROCESSORS

Customer has authorized the use by Company of the subprocessors detailed at https://www.optimizely.com/trust-center/privacy/sub-processors/ which are applicable to the Software Services being provided by Company to Customer.

EXHIBIT 2 – Details of Processing, Categories of Data and Data Subjects

Nature and Purpose of Processing

Company will Process Personal Data as necessary to perform the Software Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Software Services.

Duration of Processing

Subject to Section 8 of the DPA, Company will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Software Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer’s prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer’s Users authorized by Customer to use the Software Services

Type of Personal Data

Customer may submit Personal Data to the Software Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localization data
- Cookie ID’s
- IP Address
- Marketing Automation System ID’s

Data Map

As described in the Section 5.2 of the DPA, Customer is to provide Company a data map of categories of personal data and data subjects. Such data map, and their subsequent updates are to be appended as part of Exhibit 2.

Sub-processors

Company may engage Sub-processors to provide parts of the Software Service. Company will ensure Sub-processors only access and use the Customer’s personal data to provide the Company’s products and services and not for any other purpose. See Annex III to the Appendix to the Standard Contractual Clauses in Exhibit 1 and https://www.optimizely.com/trust-center/privacy/sub-processors/.

EXHIBIT 3 – Supplementary Measures

In light of the Schrems II decision of the CJEU (case C-311/18) according to which the use of the Standard Contractual Clauses may require supplementary measures to ensure that an adequate level of data protection according to GDPR exists when transferring personal data to third countries, the Parties have agreed the following.

1. *General Provisions*

The provisions of this Exhibit 3 apply to supplement the Standard Contractual Clauses that apply to this DPA. In addition, the provisions of Section 2 apply under this DPA generally.

2. *Geofencing*

2.1. Company has implemented processes and controls that enable it to restrict the transfer of Personal Data to one or more jurisdictions or regions in which it, its Affiliates and Sub- processors operate ("Geofencing") where the relevant database in which the Personal Data is stored has either been:

2.1.1. identified by Customer and notified to Company (through the process described at www.optimizely.com/trust-center/privacy/geofencing) as requiring Geofencing; or

2.1.2. identified by Company, its Affiliates and Sub- processors as containing Personal Data which requires Geofencing;

in order to comply with any restrictions and/or prohibitions on transfer required by Data Protection Laws and Regulations. The relevant processes and controls that implement the Geofencing restriction prevent:

2.1.3. Company and its Affiliates from hosting such Personal Data in the relevant jurisdictions or regions; and/or

2.1.4. Company Sub-processors in the relevant jurisdictions or regions from accessing or otherwise Processing the Personal Data in the course of providing Software Services.

Details of the Geofencing options can be found at www.optimizely.com/trust-center/privacy/geofencing and these may be updated from time to time by Company.

2.2. In relation to Geofencing, Customer agrees that:

2.2.1. as Controller, it is its sole responsibility to identify and notify Company all databases which contain Personal Data that will be Processed under this DPA to which Geofencing restrictions are required. Company shall be entitled to implement and adhere to any Geofencing restrictions so notified. Unless or until such notification is made then Company shall be entitled to Process such Personal Data in accordance with the provisions of Section 3.1.5 of this DPA without Geofencing restriction;

2.2.2. if Company, any Affiliate or Sub-processor identifies a dataset which contains Personal Data in the course of providing support services which it considers should be subject to a Geofencing restriction then it shall be entitled to apply such a restriction and to take such steps as are required to implement it. Where a Geofencing restriction is applied pursuant to this Section 2.2.2 of Exhibit 3, Customer will be notified promptly and Company shall be entitled to adhere to it; and

2.2.3. Where a Geofencing restriction is applied, Customer shall not issue an instruction to Company, any Affiliates or Sub- processors that would require them to contravene it and Company shall not be in breach of the Agreement (including this DPA) in circumstances where it does not comply with such an instruction.

3. *Other Supplementary Measures*

3.1. The parties agree to closely cooperate in good faith to identify and, as the case may be, agree any further additional supplementary measures (e.g., the improvement of existing (or the implementation of additional) technical and organizational security measures) in connection with the processing of Personal Data by Company under the DPA which may be appropriate in the context of the criteria stipulated in the Schrems II decision.

3.2. The parties agree that Customer's right to monitor and audit Company's obligations under the DPA (including the Standard Contractual Clauses) also extends to the Company's obligations under this Exhibit 3.

3.3. If and to the extent required in the normal course of providing the Software Services covered by the DPA, Customer consents to Company accessing Personal Data transmitted in plain text.

4. *Additional Obligations of Customer*

4.1. In addition to the requirements of clause 8.3 of the under the Standard Contractual Clauses contained in Exhibit 1, Customer is obliged, when transferring any type of Personal Data, to inform data subjects in accordance with Art. 13 and 14 GDPR that their data are transmitted to a third country not providing adequate protection within the meaning of the GDPR.

4.2. If Customer receives notice under clause 15 of the Standard Contractual Clauses contained in Exhibit 1 from Company, Customer shall inform the concerned data subject(s) without undue delay about any such legally binding request for disclosure of the Personal Data by a law enforcement, national security or any other authorities ("**Public Authority**"), unless informing the data subject proves impossible for Customer or prohibited by law.

5. *Additional Obligations of Company*

5.1. Upon request and to the extent not prohibited by law, Company will inform Customer in general terms about the access requests received from Public Authorities concerning personal data processed under the DPA, such information to consist at least of the number of requests, the nature of requested data, the legal basis for such requests and the requesting bodies unless the provision of such information proves impossible for Company is otherwise legally prohibited. In the latter case, Section 4.1 of this Exhibit 3 shall apply accordingly.

5.2. Upon request, Company shall provide Customer with all information, documentation and reasonable assistance as required enabling Customer to comply with the requirements for the transfer of personal data to Company pursuant to Art. 44 et. seq. GDPR (including any official guidance by EU Supervisory Authorities and relevant court decisions).

5.3. In accordance with clause 14 of the Standard Contractual Clauses in Exhibit 1, Company confirms that it has no reason to believe, at the time of entering into the Clauses, in the existence of any relevant local laws and practices that would have a substantial adverse effect on the terms provided for under Exhibit 1 (as applicable) and Appendix 3.

5.4. Company undertakes to regularly review and assess the applicable laws and regulations governing access to Personal Data by a Public Authority, as well as the safeguards and legal recourses in place under applicable laws and regulations to protect data subjects, and as soon as practicably possible to inform Customer in the case of a change in such applicable laws and regulations that would materially adversely impact rights and interests of data subjects and the level of protection for the Personal Data.

5.5. Company agrees that to the extent applicable to the Software Services provided by the Company (i) it has not and will not purposefully create back doors or similar programming that could be used by Public Authorities to access the system and/or Personal Data, (ii) it has not and will not purposefully create or change its business processes in a manner that facilitates access by Public Authorities to Personal Data or systems, and (iii) it is not aware of a requirement under national law or government policy requiring Company to create or maintain back doors or to facilitate access to Personal Data or systems by Public Authorities or for Company to be in possession or to hand over to Public Authorities the encryption key in this context. Notwithstanding other applicable rights of Customer, Customer shall have the right to immediately terminate the DPA and the Agreement if Company acts in violation of this Section 5.5.

6. *Third-party Beneficiary Clause*

6.1. Data subjects can enforce against Company as third-party beneficiaries under this Section 6 to this Exhibit 3 as well as Sections 1, 3.5 and 3.6 under the conditions stipulated in clause 3 (a) of the Standard Contractual Clauses in Exhibit 1.