MasterControl
Data Processing Addendum

This Data Processing Addendum ("**DPA**") is incorporated into and is subject to the terms and conditions of the current written or electronic agreement, as well as any other related order forms or statements of work (collectively, the "**Agreement**") between the entity identified as the "Client" in the Agreement (referred to herein as "**Customer**") and MasterControl Solutions, Inc or its Affiliates ("**MasterControl**") (each a "**Party**" and collectively "**Parties**"). All capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement.

This DPA reflects the agreement between MasterControl and Customer with regard to the processing of Customer Personal Data on behalf of the Customer as part of MasterControl's provision of software as a service ("**SaaS**") solutions and other services, including support and professional services as more particularly described in the Agreement (individually and collectively, the "**Services**").

By signing the Agreement, Customer hereby accepts this DPA on behalf of itself and in the name and on behalf of its Affiliates, if and to the extent MasterControl processes Customer Personal Data, provided that such Affiliates have not signed their own separate agreement with MasterControl ("**Authorized Affiliates**"). For the purposes of this DPA only, and except where the context otherwise requires, the term "Customer" will include Customer and Authorized Affiliates.

The Parties agree as follows:

1. **Definitions**

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity. "**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" will be construed accordingly.

"**Customer Data**" means the content and/or any other data (whether personal data or not) provided to MasterControl by (or on behalf of) Customer or its End Users through the Services.

"**Customer Personal Data**" means any Customer Data that is protected as "personal data" under Data Protection Laws that MasterControl processes on behalf of Customer in the course of providing the Services, as more particularly described in **Annex A** of this DPA.

"**Data Protection Laws**" means all worldwide data protection and privacy laws and regulations, applicable to a Party's processing of Customer Personal Data under or in connection with the Agreement, including where applicable (i) 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, and repealing Directive 95/46/EC ("**GDPR**"); (ii) Directive 2002/58/EC concerning the Processing of personal data and the protection of privacy in the electronic communications sector; (iii) any applicable national implementations of (i) and (ii); (iv) GDPR as it forms part of United Kingdom law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018 (together, "**UK Privacy Laws**"); and (v) the Swiss Federal Data Protection Act ("**Swiss DPA**"); in each case, as may be amended, superseded or replaced.

"**Europe**" means, for the purposes of this DPA, the European Economic Area ("**EEA**") and/or its member states, the United Kingdom and/or Switzerland.

"**End User**" means an individual that Customer authorizes to access and use the Services

"**Purposes**" shall mean the data processing purposes described in Annex A of this DPA.

"**Restricted Transfer**" means: (i) where the GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where UK Privacy Laws apply, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data on systems managed by or otherwise controlled by MasterControl but does not include any Unsuccessful Security Incident.

"**Standard Contractual Clauses**" means the Standard Contractual Clauses as set out in the European Commission's Decision (EU) 2021/914 of 4 June 2021 (available online at:https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf (europa.eu)).

"**Sub-processor**" means any data processor engaged by MasterControl to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or MasterControl's Affiliates.

"**UK Addendum**" means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner's Office under S119(A) of the UK Data Protection Act 2018, as updated or amended from time to time.

"**Unsuccessful Security Incident**" means an unsuccessful attempt or activity that does not compromise the security of Customer Personal Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

The terms "**data subject**" "**personal data**", "**controller**", "**processor**", "**processing**" and "**supervisory authority**" shall have the meaning given to them in GDPR, and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.

2. Scope and Applicability of this DPA

2.1 This DPA applies where and only to the extent that MasterControl processes Customer Personal Data that is protected by Data Protection Laws applicable to MasterControl as a processor (or sub-processor) on behalf of the Customer in the course of providing Services pursuant to the Agreement.

2.2 Notwithstanding expiry or termination of the Agreement, this DPA and any Standard Contractual Clauses (if applicable) will remain in effect until, and will automatically expire upon, deletion of all Customer Personal Data by MasterControl as described in this DPA.

2.3 Where Customer is a California business covered by the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, including any related implementing regulations (collectively, "**CCPA**"), the terms of Annex B (CCPA Data Process Addendum) shall additionally apply.

2.4 Where Customer Personal Data pertains to data subjects in India, the terms of Annex C (India Data Protection Addendum) shall additionally apply.

3. **Roles and Scope of Processing**

3.1 **Role of the Parties**. As between Customer and MasterControl, Customer is the controller (whether itself a controller or acting on behalf of a third-party controller) of Customer Personal Data, and MasterControl shall process Customer Personal Data only as a processor acting on behalf of Customer as described in **Annex A** (Details of Processing) of this DPA. Any processing of personal data under the Agreement shall be performed in accordance with applicable Data Protection Laws. However, MasterControl is not responsible for compliance with any Data Protection Laws applicable to Customer or Customer's industry that are not generally applicable to MasterControl as a service provider.

3.2 **Customer Instructions**. MasterControl will process Customer Personal Data only in accordance with Customer's documented lawful instructions. For these purposes, Customer instructs MasterControl to process Customer Personal Data for the Purposes, except where otherwise required by applicable law. The parties agree that the Agreement (including this DPA) sets out the Customer's complete and final instructions to MasterControl in relation to the processing of Customer Personal Data. Additional processing outside the scope of these instructions (if any) will require prior written agreement between Customer and MasterControl. If Customer is itself processor acting on behalf of a third-party controller (or other intermediary): (i) Customer represents and warrants to MasterControl that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of MasterControl as another processor, have been authorized by the relevant controller; (ii) Customer will serve as the sole point of contact for MasterControl with regard to any third party controllers of the Customer Personal Data; (iii) MasterControl need not interact directly with (including seek any authorisations directly from) any such third party controllers (other than through regular provision of the Services to the extent required by the Agreement); and (iv) where MasterControl would (including for the purposes of the Standard Contractual Clauses) otherwise be required to provide information, assistance, cooperation, or anything else to such third party controllers, MasterControl may provide it solely to Customer. Notwithstanding the foregoing, MasterControl is entitled to follow the instructions of such third party with respect to such third party's Customer Personal Data instead of Customer's instructions if MasterControl reasonably believes this is legally required under the circumstances.

3.3 **Notification Obligations Regarding Customer Instructions**. MasterControl shall promptly notify Customer in writing, unless prohibited from doing so under Data Protection Law, if: (a) it becomes aware or believes that any data processing instruction from Customer violates Data Protection Law; or (b) it is unable to comply with Customer's data processing instructions.

4. **Subprocessing**

4.1 **Authorized Sub-processors**. Subject to MasterControl complying with this Section 4 (Subprocessing), Customer agrees that MasterControl may engage Sub-processors to process Customer Personal Data on Customer's behalf. The Sub-processors currently engaged by

MasterControl and authorized by Customer are MasterControl's Affiliates and the third parties listed here www.mastercontrol.com/privacy/sub-processors (the "**Sub-processor List**").

4.2 **Sub-processor Obligations**. MasterControl will: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-processor; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause MasterControl to breach any of its obligations under this DPA.

4.3 **Changes to Sub-processors**. MasterControl shall notify Customer if it adds or removes Sub-processors at least ten (10) days prior to any such changes by updating the Sub-processor List and providing Customers with a mechanism to obtain notice of the update). Customer may object in writing to MasterControl's appointment of a new Sub-processor within ten (10) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the Parties will discuss such concerns in good faith with a view to achieving resolution. If MasterControl cannot provide an alternative Sub-processor, or the Parties are not otherwise able to achieve resolution as provided in the preceding sentence within a reasonable period not to exceed sixty (60) days, Customer as its sole and exclusive remedy, may terminate the relevant part of the Agreement (including this DPA) regarding those Services which cannot be provided by MasterControl without the use of the Sub-processor concerned without liability to either Party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

5. **Security**

5.1 **Security Measures**. MasterControl shall implement and maintain appropriate technical and organizational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data, in accordance with MasterControl's security standards described in the MasterControl Security Addendum found here www.mastercontrol.com/privacy/security-measures (or such other successor URL as may be notified to Customer) ("**Security Measures**"). MasterControl shall ensure that any person who is authorized by MasterControl to process Customer Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.2 **Updates to Security Measures**. Customer is responsible for reviewing the information made available by MasterControl relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that MasterControl may update or modify the Security Measures from time to time provided that such updates and modifications do not result in a material degradation of the overall security of the Services subscribed to by Customer.

5.3 **Security Incident Response**. In the event of a Security Incident, MasterControl shall: (i) notify Customer without undue delay, and in any event such notification shall, where feasible, occur no later than 72 hours from MasterControl becoming aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) MasterControl shall promptly take all reasonable steps to contain, investigate, and mitigate any Security Incident. MasterControl's notification of or response to a Security Incident under this Section 5.3 (Security Incident Response) will not be construed as an

acknowledgment by MasterControl of any fault or liability with respect to the Security Incident. Unless otherwise required under Data Protection Law, the Parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected data subjects and/or notices to the relevant supervisory authorities.

6. **Security Reports and Audits**

6.1 **Audit Rights**. MasterControl shall make available to Customer information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits or inspections of MasterControl-owned and controlled data center facility that processes Customer Personal Data. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including this Section 6.1 and where applicable, the Standard Contractual Clauses) by instructing MasterControl to comply with the audit measures described in Sections 6.2 and 6.3 below.

6.2 **Security Information**. Upon written request, MasterControl shall supply (on a confidential basis) reasonable documentation evidencing MasterControl's compliance with its obligations under this DPA to Customer. If such documentation does not, in Customer's reasonable judgement, provide sufficient information to confirm MasterControl's compliance with this DPA, then MasterControl shall also provide written responses (on a confidential basis) to reasonable requests for information made by Customer, including responses to information security and audit questionnaires that are necessary to confirm MasterControl's compliance with this DPA, provided that Customer shall not exercise this right more than once per calendar year. Notwithstanding the foregoing, Customer may also exercise such audit right in the event Customer is expressly requested or required to provide this information to a data protection authority.

6.3 **Virtual Audit**: Where required by applicable Data Protection Law or where a competent data protection authority requires this under applicable Data Protection Law, MasterControl shall in addition allow Customer or another auditor approved by the Parties to (at Customer's expense) audit compliance with this DPA and to inspect MasterControl's documents and electronic data relating to the processing of Customer Personal Data by MasterControl, provided that: (i) Customer shall not exercise this right more than once every twelve (12) months; (ii) such additional audit enquiries shall not unreasonably impact in adverse manner MasterControl's regular operations and do not prove to be incompatible with applicable legislation or with the instructions of a competent authority. It should be noted that audits are performed virtually, as client data is not stored directly at MasterControl facilities. Since inspection of the storage equipment is not possible, audits can feasibly be performed in a virtual format to reduce expenses and to provide the most efficient audit possible. Before the commencement of any audit activities, Customer and MasterControl shall mutually agree upon the scope, timing, and duration of the audit.

7. **Customer Responsibilities**

7.1 **Security**. Customer agrees that, without prejudice to MasterControl's obligations under Section 5.1 (Security Measures) and Section 5.4 (Security Incident Response):

(a) Customer is responsible for its use of the Services, including making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data, securing its account authentication credentials, managing its data back-up strategies, and protecting the security of Customer Personal Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Personal Data;

(b) Customer shall be solely responsible for ensuring Customer Personal Data accessed, maintained or stored by MasterControl's personnel while on the Customer's facilities and/or otherwise accessed or processed by MasterControl's personnel on computer systems or other electronic equipment controlled by Customer during the provision of the Services is processed in compliance with Customer's data protection and security obligations under applicable Data Protection Laws and any associated policies, codes of practices and/or procedures relating to any End User, worker, customer, Customer, or supplier of the Customer; and

(c) MasterControl has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of MasterControl's and its Sub-processors' systems (for example, offline or on-premise storage).

7.2 **Customer Processing of Personal Data**. Customer is solely responsible for the lawfulness of Customer Personal Data processing under or in connection with the Agreement. Customer represents and warrants that: (i) it has provided, and will continue to provide, all notice and obtained, and will continue to obtain, all consents, permissions and rights necessary under Data Protection Laws for MasterControl to lawfully process Customer Personal Data on Customer's behalf and in accordance with its instructions; (ii) it has complied with all applicable Data Protection Laws in the collection and provision to MasterControl and its Sub-processors of such Customer Personal Data; and (iii) it shall ensure its processing instructions comply with applicable laws (including Data Protection Laws) and that the processing of Customer Personal Data by MasterControl in accordance with the Customer's instructions will not cause MasterControl to be in breach of applicable Data Protection Laws.

8. **Co-operation and Data Protection Impact Assessments**

8.1 **Data Subject Requests**. To the extent Customer is unable to independently retrieve, access or delete the relevant Customer Personal Data within the Services, MasterControl shall (at Customer's request and expense and taking into account the nature of the processing) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Customer Personal Data under the Agreement. In the event that any request from individuals or applicable data protection authorities is made directly to MasterControl where such request identifies Customer, MasterControl shall not respond to such communication directly without Customer's prior authorization (except to direct the data subject to MasterControl), unless legally compelled to do so, and instead, after being notified by MasterControl, Customer shall respond. If MasterControl is required to respond to such a request, MasterControl will promptly notify Customer and provide it with a copy of the request, unless legally prohibited from doing so. The Parties agree that the certification of deletion that is described in Clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by MasterControl to Customer only upon Customer's written request.

8.2 **Record Keeping**. Customer acknowledges that MasterControl is required under Data Protection Laws to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which MasterControl is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, Customer will, where requested, provide such information to MasterControl via means provided by MasterControl, and will ensure that all information provided is kept accurate and up-to-date.

8.3 **DPIAs**. To the extent MasterControl is required under applicable Data Protection Laws, MasterControl shall (at Customer's request and expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

9. **Return or Deletion of Data**

9.1 Upon Customer's request, or upon termination or expiry of the Agreement, MasterControl shall destroy or return to Customer Personal Data in its possession or control. This requirement shall not apply to the extent that MasterControl is required by any applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal Data MasterControl shall securely isolate and protect from any further processing and eventually delete in accordance with MasterControl's deletion policies, except to the extent required by such law. The Parties agree that the certification of deletion that is described in Clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by MasterControl to Customer only upon Customer's written request.

10. **Data Transfers**

10.1 **Location of Processing**. Personal data that MasterControl's processes under the Agreement may be processed in any country in which MasterControl, its Affiliates and authorized Sub-processors maintain facilities to perform the Services. Where GDPR applies, MasterControl shall not process or transfer (directly or via onward transfer) Customer Personal Data (not permit such data to be processed or transferred) outside Europe in a country that does not offer adequate protection for personal data (within the meaning of applicable Data Protection Laws) (a "**Third Country**"), unless it first takes such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Laws.

10.2 **Standard Contractual Clauses**. The Parties agree that where transfer of Customer Personal Data from Customer to MasterControl is a Restricted Transfer and Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be subject to the Standard Contractual Clauses, which shall be deemed incorporated by reference and form an integral part of this DPA. For the purposes of the Standard Contractual Clauses, the Parties agree that:

(a) In relation to transfers of Customer Personal Data subject to the GDPR, the Standard Contractual Clauses shall apply as follows:

(i) MasterControl is the "data importer" and Customer is the "data exporter";

(ii) Module Two (controller to processor) or Module Three (processor to processor) terms will apply (as applicable);

(iii) in Clause 7, the optional docking clause will apply;

(iv) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes will be as set out in Section 4.3 (Changes to Sub-processors) of this DPA;

(v) in Clause 11, the optional language will not apply;

(vi) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Irish law;

(vii) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(viii) Annex I of the Standard Contractual Clauses shall be deemed completed with the information set out in Annex A of this DPA; and

(ix) subject to Sections 5.1 and 5.2 of this DPA, Annex II of the Standard Contractual Clauses shall be deemed completed with the information set out in the Security Measures;

(b) In relation to transfers of Customer Personal Data protected by UK Privacy Laws, the Standard Contractual Clauses: (i) shall apply as completed in accordance with paragraph (a) above; and (ii) shall be deemed amended as specified by the UK Addendum, which shall be deemed executed by the Parties and incorporated into and form an integral part of this DPA. In addition, Tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Annexes A and B of this DPA and Table 4 in Part 1 shall be deemed completed by selecting "neither party".

(c) In relation to transfers of Customer Personal Data protected by the Swiss DPA, the Standard Contractual Clauses shall also apply in accordance with paragraph (a) above, with the following modifications:

(i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

(iii) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland", or "Swiss law";

(iv) the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

(v) Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection Information Commissioner;

(vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";

(vii) in Clause 17, the Standard Contractual Clauses shall be governed by the laws of Switzerland; and

(viii) Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

(d) It is not the intention of either Party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses. Accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict.

11. **Change in Laws**

11.1 Where there is a change in applicable Data Protection Laws that materially or adversely impacts MasterControl's continued provision of the Services (including its costs in providing the Services), MasterControl shall notify the Customer in writing and the Parties shall discuss in good faith what changes may be necessary to the Agreement (including this DPA) and/or the Services (including, without limitation, the fees payable by the Customer to MasterControl for the Services) in order to enable MasterControl to continue providing the Services in accordance with the Agreement (including this DPA).

11.2 In the event that ongoing provision of the Services is operationally, technically or economically infeasible, or if the Parties are unable to agree such changes as may be necessary, then each Party shall have the right without liability to terminate the Agreement for convenience.

12. **Limitation of Liability**

12.1 Each Party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the Standard Contractual Clauses) shall be subject to the exclusions and limitations of liability set forth in the main body of the Agreement.

12.2 Any claims against MasterControl or its Affiliates under or in connection with this DPA (including, where applicable, the Standard Contractual Clauses) shall be brought solely against the Customer entity that is a party to the Agreement.

12.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

13. **Rights of Authorized Affiliates.**

13.1 Where an Authorized Affiliate becomes a party to the DPA with MasterControl, it will to the extent required under applicable Data Protection Law be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

(a) Except where applicable Data Protection Law require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against MasterControl directly by itself, Parties agree that (i) solely the Customer that is the contracting party to the Agreement will exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement will 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 subsection (b) below).

(b) The Parties agree that the Customer that is the contracting party to the Agreement will, when carrying out an on-site audit of the procedures relevant to the protection of Customer Personal Data, take all reasonable measures to limit any impact on MasterControl 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.

14. **Relationship with the Agreement**

14.1 The Parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Services.

14.2 Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that MasterControl shall have a right to use data relating to the operation, support and/or use of the Services ("**Service Data**") for its legitimate business purposes, such as billing, account management, technical support and troubleshooting, product development and sales and marketing. To the extent any MasterControl Data is considered personal data, MasterControl shall process such data in accordance with applicable Data Protection Laws.

14.3 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict or inconsistency between this DPA and the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) Standard Contractual Clauses (where applicable); then (b) this DPA; and then (c) the main body of the Agreement.

14.4 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

Annex A

Data Processing Description / Description of Transfer

Annex 1(A) List of Parties:

Data Exporter	**Data Importer**
Name: The party identified as the "Customer" in the DPA.	Name: MasterControl
Address: The address for the Customer specified in the Agreement.	Address: 6350 South 3000 East, Cottonwood Heights, Utah 84121, USA
Contact Person's Name, position and contact details: The Customer point of contact provided in the relevant order form.	Contact Person's Name, position and contact details: MasterControl Privacy Team privacy@mastercontrol.com
Activities relevant to the transfer: See Annex 1(B) below	Activities relevant to the transfer: See Annex 1(B) below
Role: Controller or Processor	Role: Processor

Annex 1(B) Description of Processing / Transfer

(a) Subject matter: The subject matter of the data processing under this DPA is the Customer Personal Data.

(b) Categories of Data Subjects: Data subjects include individuals about whom data is provided to MasterControl via the Services (by or at the direction of) the Customer or by End Users, and which may include, but is not limited, the following types of data subjects:

(i) Prospects, customers, business partners and vendors of Customer (who are natural persons)

(ii) Employees or contact persons of Customer's prospects, customers, business partners and vendors

(iii) Employees, agents, advisors, freelancers of Customer (who are natural persons)

(c) Types of Personal Data: Personal data submitted, stored, sent or received by Customer or end users via the Services may include mobile device o/s advertising identifiers, MasterControl pseudonymous identifiers, and IP addresses collected via computers and mobile devices.

Personal data submitted, stored, sent or received by and applicable to Customer or Customer's employees, agents, or contractors that are necessary for the provision of the

Services include: name, title, company postal address, email address, telephone number, and billing information.

Additionally, the Customer may submit Customer Personal Data to the 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 types of personal data:

(i) First and last name
(ii) Title
(iii) Position
(iv) Employer
(v) Contact information (company, email, phone, physical business address)
(vi) ID data
(vii) Employee training data
(viii) Professional life data
(ix) Personal life data
(x) Connection data
(xi) Localization data

Customer Personal Data fields may also be configured as part of the implementation of the Services or as otherwise permitted within the scope of the Services.

(d) Special Categories of Personal Data (if applicable): The Customer may also include "special categories of personal data" or similarly sensitive personal data (as described or defined in Data Protection Laws) in Customer Personal Data, the extent of which is determined and controlled by the Customer in its sole discretion.

(e) Frequency of the Transfer: The Customer Personal Data will be transferred on a continuous basis in accordance with the Customer's instructions as described in this DPA.

(f) Nature of processing: MasterControl is a provider of enterprise cloud hosted document and quality management solutions, as further described in the Agreement.

(g) Purpose: Customer Personal Data may only be processed by MasterControl for the following purposes: (i) as necessary for the performance of the Services and MasterControl' obligations under and pursuant to the Agreement (including this DPA); (ii) processing initiated by End Users in their use of the Services; and (iii) any other purposes of processing of Customer Personal Data agreed upon between the Parties in the relevant order form, statement of work or any other document of the Agreement (the "**Purposes**").

(h) Duration and retention period: The (a) term of the Agreement; and (b) any period after the termination or expiry of the Agreement during which MasterControl processes Customer Personal Data, until MasterControl has deleted, destroyed or returned such Customer Personal Data in accordance with the terms of the Agreement (including this DPA).

Annex 1(C) Competent Supervisory Authority

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

MasterControl

Annex B

CCPA Data Processing Addendum

WHEREAS, the CCPA imposes a duty on businesses to include specific terms in agreements with its service providers in order to protect the personal information collected from such businesses' workforce members who are residents of California (hereafter, "**California Employee HR Data**"). Under the CCPA, a service provider is a person that processes personal information on behalf of a covered business and receives that information from or on behalf of the business for a business purpose and under a written contract containing specific terms; and

WHEREAS, The Parties agree that Customer is a California business covered by the CCPA and therefore the personal information collected from Customer's California workforce members or potential workforce members is protected under the CCPA. The Parties further agree that MasterControl is a service provider to Customer as defined under the CCPA, and accordingly, MasterControl will provide the services specified in the Services Agreement and process any California Employee HR Data in accordance with the Services Agreement.

1. Additional Terms. The Parties agree to the following additional terms to the Services Agreement.

   a. Customer discloses its California Employee HR Data to MasterControl only for the limited and specific business purpose outlined in the scope of work of the Services Agreement; MasterControl may only process the California Employee HR Data for that specific business purpose.

   b. MasterControl agrees to comply with applicable CCPA obligations in the processing of Customer's California Employee HR Data, including providing the same or similar level of privacy protection for the California Employee HR Data that Customer must provide under the CCPA. For the avoidance of doubt, such privacy protection must include, as required by the CCPA, implementing reasonable security procedures and honoring any consumer opt-out requests that the business forwards to MasterControl that relate to information held by MasterControl in accordance with the services provided to Customer, subject, however, to the terms and provisions of paragraph (g) below.

   c. MasterControl shall make available to Customer information reasonably necessary to demonstrate compliance with this Addendum. Requests for information must be made in writing and must specify specific items needed to demonstrate compliance. MasterControl shall provide this information within 30 days of receipt of the request. MasterControl shall allow for and contribute to audits or inspections of MasterControl facilities that process California Employee HR Data obtained under the Services Agreement, in accordance with MasterControl's role as a service provider to Customer under the CCPA. Customer acknowledges that MasterControl is regularly audited against ISO 27001 standards by independent third-party auditors and/or internal auditors. Upon written request, MasterControl will supply the most current ISO certifications. MasterControl will, in addition, allow Customer or another auditor approved by the parties and at Customer's expense, the right to audit compliance with this Addendum and to inspect MasterControl's documentation and electronic data relating to the processing of California Employee HR Data by MasterControl, provided that:

      (i) Customer shall not exercise this right more than once every twelve (12) months;

(ii) Such additional audit inquiries shall not unreasonably impact in any adverse manner MasterControl's regular operations and will not prove to be incompatible with applicable legislation or with the instructions of a competent authority; and

(iii) Before the commencement of any such additional audit inquiries, Customer and MasterControl shall mutually agree on the scope and date of the audit with the understanding that MasterControl only agrees to host half-day (4-hour) virtual audits.

d. MasterControl permits Customer to take reasonable action to stop and remediate MasterControl's unauthorized use of California Employee HR Data obtained under the Services Agreement.

e. MasterControl agrees to promptly notify Customer if MasterControl can no longer meet its CCPA obligations.

f. MasterControl is specifically prohibited from the following:

i. "Selling" or "sharing" (as such terms are defined in the CCPA) California Employee HR Data obtained under the Services Agreement;

ii. Retaining, using, or disclosing California Employee HR Data obtained under the Services Agreement for any purpose except the Services Agreement's specified business purposes or as the CCPA otherwise permits, including for any other commercial purpose;

iii. Retaining, using, or disclosing California Employee HR Data obtained under the Services Agreements outside of the Parties' direct relationship, unless the CCPA expressly permits the use. Notwithstanding anything to the contrary, Customer agrees that MasterControl may engage others to assist in providing the services under the Services Agreement ("Sub-Service Providers"). The Sub-Service Providers currently engaged by MasterControl and authorized by Customer are MasterControl's Affiliates and the third parties listed here: www.mastercontrol.com/privacy/sub-processors. Each authorized Sub-Service Provider shall agree in writing to obligations substantially similar to MasterControl's obligations under this Addendum. In addition, MasterControl shall be permitted to retain one copy of the California Employee HR Data for the purpose of complying with any internal document retention policies and establishing compliance with any applicable laws or regulations, and for defending or maintaining any litigation relating to this Addendum or the Services Agreement, in each case provided that such California Employee HR Data shall remain subject to the confidentiality and non-use obligations set forth herein in accordance with the terms hereof; and

iv. Combining or updating California Employee HR Data obtained under the Services Agreement with any personal information MasterControl obtains through other sources or from MasterControl's consumer interactions outside of the Services Agreement, unless the CCPA expressly permits the activity.

g. MasterControl provides Customer with tools to enable Customer to respond to a CCPA consumer rights request whereby an individual requests to exercise certain rights under the CCPA. To the extent Customer is unable to respond to a CCPA consumer rights request using these tools, MasterControl will provide reasonable assistance and cooperation to Customer in responding to such CCPA consumer rights requests.

h. Customer agrees that, without prejudice to MasterControl's obligations under this Addendum and the Services Agreement, Customer is responsible for its use of the services provided by MasterControl under the Services Agreement, including: (i) securing its account authentication credentials; (ii) managing its data back-up strategies; (iii) protecting the security of California Employee HR Data when in transit to and from MasterControl; and (iv) taking any appropriate steps to securely encrypt or backup any California Employee HR Data. For the avoidance of doubt, MasterControl has no obligation to protect California Employee HR Data that Customer elects to store or transfer outside of MasterControl's systems (for example, offline or on-premise storage).

Annex C

India Data Processing Addendum

This India Data Processing Addendum incorporates additional legal requirements, rights and obligations applicable to the processing of personal data in India and shall be read together with the terms of the DPA. In the event of a conflict between the terms of this India Data Processing Addendum and the DPA or the Agreement, the terms of this India Data Processing Addendum shall prevail.

The Parties agree as follows:

1. "**Data Protection Laws**" shall also include all Applicable Laws governing the protection of personal data and the collection, processing, storage, use and/or application of personal data or privacy of an individual including but not limited to the (Indian) Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, the Digital Personal Data Protection Act, 2023 and rules framed thereunder (as and when notified), the Information Technology Act, 2000 and rules notified thereunder.

2. Without prejudice to Section 5.3 of the DPA, the Customer and MasterControl agree that they shall assist each other to comply with their respective obligations to notify appropriate regulators and/or Persons within the prescribed statutory periods, regarding Security Incidents as required under Data Protection Laws.

3. Section 8.1 of the DPA is replaced as follows:

   Data Subject Requests. Subject to Customer's instructions, and where Customer is unable to independently action any requests from data subjects to exercise their rights, MasterControl shall assist Customer in responding to such requests as available under Data Protection Laws. Upon receiving a request directly from a data subject, MasterControl shall not respond to such communication or request without Customer's prior authorization (except to direct the data subject to Customer), unless legally compelled to do so. If MasterControl is required to respond to such a request, MasterControl will promptly notify Customer and provide it with a copy of the request, unless legally prohibited from doing so.

4. Section 9.1 of the DPA is replaced as follows:

   9.1 Upon Customer’s request, or upon the data subject's request, or upon the termination or expiry of the Agreement, whichever is earlier, MasterControl shall destroy or return to Customer, Customer Personal Data in its possession or control. This requirement shall not apply to the extent that (a) data is retained for a limited time post-termination or expiry to serve the specified purpose of processing or (b) MasterControl is required by any applicable law to retain some or all of the Customer Personal Data.

5. Section 10 of the DPA is replaced as follows:

   10. Customer Personal Data that MasterControl processes under the Agreement may be processed in any country in which MasterControl, its Affiliates and authorized Sub-processors maintain facilities to perform the Services. If Customer requires MasterControl to transfer any Customer Personal Data within India, or to other jurisdictions as permitted under Data Protection Laws, Customer shall ensure and provide MasterControl with a confirmation that such transfer shall be in accordance with Data Protection Laws.

6. For the purposes of Annex A 1(C) the data exporter's competent supervisory authority will be determined in accordance with the Data Protection Laws.