Medius Data Processing Addendum

This data processing addendum (the **"DPA"**) forms part of the Medius Master Cloud Subscription and Services Agreement, the Supplier Portal Terms of Use or any other written agreement between any company within the Medius group and Customer (the "**Agreement**") to reflect the parties agreement with regard to Processing of Personal Data and contains certain terms relating to data protection, privacy, and security in accordance with the requirements of the GDPR, the UK GDPR, the CCPA, and other laws or regulations relating to Medius's processing of Personal Data on Customer's behalf, where applicable. In the event that there is a conflict between any of these Data Protection Laws and Regulations, the parties shall comply with the more onerous requirement or higher standard.

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

In the course of providing services to Customer pursuant to the Agreement, Medius 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 in good faith.

1. DEFINITIONS

The following terms shall have the following meanings in this Data Processing Addendum.

1.1 **"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control", or purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

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

1.3 **"CCPA"** means the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 et seq.), as amended in 2020 by the California Privacy Rights Act.

1.4 "**Data Protection Laws and Regulations**" means: i) the GDPR and all other applicable EU, EEA or European single market Member State laws or regulations or any update, amendment or replacement of same that apply to processing of personal data under the Agreement; (ii) all U.S. laws and regulations that apply to processing of personal data under the Agreement including but not limited to CCPA; (iii) all laws and regulations that apply to processing of personal data under the Agreement from time to time in place in the United Kingdom (including the UK GDPR), and the terms "controller", "process", "processing", "processor", "supervisory authority" have the same meanings as in the GDPR or the UK GDPR and with respect to CCPA (as defined above) as applicable, the Parties hereby agree that Medius is a "Service Provider" and Customer is the "Business", as defined under the CCPA with respect to Personal Information (as defined under the CCPA).

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

1.6 **"GDPR"** means 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, and repealing Directive 95/46/EC (General Data Protection Regulation). References in this DPA to GDPR will to the extent applicable be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).

1.7 **"Personal Data**" means any information relating to an identified or identifiable natural person where such data is Customer's data.

1.8 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

1.9 **"Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automated means (such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction).

1.10 **"Processor"** means the entity which Processes Personal Data on behalf of the Controller.

1.11 **"Restricted Transfer"** means i) a transfer of Personal Data from Customer to Medius or ii) an onward transfer of Personal Data from Medius to a Sub-processor, in each case, where such transfer would be prohibited by Data Protection Laws and Regulations in the absence of the Standard Contractual Clauses, the UK Addendum or any other transfer mechanism referenced in chapter 5 of the GDPR. For the avoidance of doubt, where a transfer of Personal Data is of a type authorised by Data Protection Laws or Regulations in the exporting country, for example in the case of transfers from within the European Union to a country (such as Switzerland or the United Kingdom) which is approved by the Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer.

1.12 **"Services"** means the Services provided to Customer under the Agreement.

1.13 **"Standard Contractual Clauses"** means the Standard Contractual Clauses pursuant to Commission Decision (EU) 2021/914 of 4 June 2021 in conjunction with the International Data Transfer Addendum to the EU Standard Contractual Clauses available at https://www.medius.com/legal/uk-addendum-to-dpa/ (the "**UK Addendum**").

1.14 **"Sub-processor"** means any Processor engaged by Medius or by Medius's Affiliate/s.

1.15 **"Supervisory Authority"** means an independent public authority which is established by an EU Member State pursuant to the GDPR.

1.16 **"UK GDPR"** means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

1.17 "**Medius**" means the Medius company with which Customer has entered into the Agreement.

1.18 "**Customer"** means the company or other legal entity that executes the Agreement with Medius.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to Medius's Processing of Personal Data on Customer's behalf, Customer is the Controller and Medius is the Processor.

2.2 **Customer's Processing of Personal Data.** Customer shall Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations and Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer collected Personal Data.

2.3 **Medius's Processing of Personal Data.** Medius 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: (a) Processing in accordance with Appendix 1 (Details of the Processing) and the Agreement; (b) Processing initiated by Users in their use of the services; and (c) Processing to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement. Medius will immediately inform Customer if any of Customer's instructions, in Medius's opinion, infringes any Data Protection Laws and Regulations. Medius shall be responsible for complying with all Data Protection Laws and Regulations applicable to Medius's provision of the Services in Medius's role as Data Processor. However, Medius is not responsible for compliance with any laws applicable to Customer's or Customer's industry that are not generally applicable to spend management information technology service providers. To the extent Medius will process Customer's data that is "Personal Information" subject to the CCPA, Medius does so as a service provider (as the term is defined in the CCPA) and acknowledge the following restrictions: a) Medius will process, retain, use, and disclose personal information, including Customer Data, for the sole purpose of providing the Services or as otherwise permitted under the Agreement, or this DPA as specified in Appendix 1 (Details of the Processing); b) Medius will not sell or share the Personal Information; c) Medius will not process, retain, use, or disclose, including to a third party for valuable consideration, Personal Information, including Customer Data, for any purpose other than for the business purposes specified in the Agreement; d) Medius will not process, retain, use, or disclose personal information, including Customer Data, for any purpose outside of the direct business relationship between Customer and Medius; and e) Medius shall provide reasonable support and response to inquiries from Customer regarding Medius's data processing obligations.

2.4 **Details of the Processing.** The subject-matter of Processing of Personal Data by Us is the performance of Services. Details about 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 Appendix 1 (Details of the Processing) to this DPA.

2.5 **Affiliates and third parties.** In case it is expressly agreed under the Agreement that Customer's Affiliates or any other third parties shall also benefit from the Services, Customer acts in this respect on behalf of and in the name of Customer's Affiliates and/or third parties in their capacity as Controllers and Customer shall to the extent necessary enter into data processing agreements with such Controllers required to allow Medius and Medius's Sub-processors to process any Personal Data as described in this DPA. Customer shall serve as a single point of contact for Medius and shall be solely responsible for the internal coordination, review and submission of instructions or requests of other Controllers to Medius and Medius shall be entitled to refuse any requests or instructions provided directly by a Controller that is not Customer. Medius shall further have no obligation to inform or notify a Controller when Medius has provided such information or notice to Customer.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Request.** Medius shall, to the extent legally permitted, promptly notify Customer if Medius 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, or any other right under the Data Protection Laws and Regulations ("**Data Subject Request**"). Taking into account the nature of the Processing, Medius 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 Customer's use of the Services, do not have the ability to address a Data Subject Request, Medius shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Medius 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 Medius's provision of such assistance.

SECURITY AND CONFIDENTIALITY

4.1 **Protection of Personal Data**. Medius shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to Customer's Personal Data), confidentiality and integrity of Customer's Personal Data. Such measures shall take into account the nature, scope, context and purposes of the Processing as well as the risks of varying likelihood and severity for the rights and freedom of natural persons. The measures shall be reviewed and updated where necessary.

4.2 **Confidentiality**. Medius shall ensure that Medius's 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 committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Medius shall take commercially reasonable steps to ensure the reliability of Medius's personnel engaged in the Processing of Personal Data and shall ensure that Medius's access to Personal Data is limited to those personnel performing Services.

SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Medius's Affiliates may be retained as Sub-processors; and (b) Medius and Medius's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services and (c) that Medius may continue to use those Sub-processors already engaged by Medius or Medius's Affiliates as at the date of this DPA, which are listed at https://www.medius.com/media/e5oew4dx/medius-sub-processors.pdf. Medius or Medius's Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer's Personal Data to the extent applicable to the nature of the services provided by such Sub-processor. Customer acknowledges and agrees that Medius may remove Sub-processors at Medius's own discretion.

5.2 **New Sub-processors**. Customer may object to Medius's use of a new Sub-processor by notifying Medius in writing within (10) business days after receipt of information of Medius's intended changes concerning the addition of a new Sub-processor. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Medius will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Medius is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the Agreement with respect only to those Services which

cannot be provided by Medius without the use of the objected-to new Sub-processor by providing written notice to Medius. Medius will refund Customer any prepaid fees covering the remainder of the term of such Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.3 **Liability.** Medius shall be liable for the acts and omissions of Medius's Sub-processors to the same extent Medius would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. NOTIFICATION OF PERSONAL DATA BREACHES AND OTHER ASSISTANCE

6.1 Medius shall notify Customer without undue delay, and where feasible, not later than 48 hours, after becoming aware of a Personal Data Breach affecting Customer's Personal Data, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects or the Supervisory Authority pursuant to article 33 of GDPR or any other applicable law or regulation to notify relevant supervisory authorities or data subjects . Medius shall investigate the Personal Data Breach and take reasonable steps to mitigate the effects and to minimize any damage resulting from the breach.

6.2 To the extent not already explicitly covered by Medius's obligations in this DPA, Medius shall assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR taking into account the nature of processing and the information available to Us.

7. RETURN AND DELETION OF PERSONAL DATA

7.1 Unless otherwise is explicitly agreed in the Agreement, Medius shall upon the expiration or termination of the Agreement or upon Customer's request, provide Customer with Customer's Personal Data in standardized format at Customer's cost. If Customer require the data in another format, Medius undertakes to investigate the possibilities to perform such export. Medius undertakes to store the Data one (1) month after the Agreement's expiration or termination or until any requested transfer of data has been performed and the data will be deleted not later than ninety (90) days thereafter unless another retention period is agreed. Notwithstanding the foregoing, Customer Data in back-ups may be retained in accordance with Medius's standard back-up routines for up to two years following termination of this Agreement, provided such back-ups are maintained in a secure manner.

RESTRICTED TRANSFERS

8.1 The Parties understand and agree that Personal Data processed in accordance with this DPA may be transferred to respectively accessed from countries outside of the EU/EEA, the UK, US and Switzerland by Us, Medius's Affiliates and Sub-processors when providing the Services in accordance with the terms of the Agreement.

8.2 For Restricted Transfers from the European Economic Area that are subject to the Standard Contractual Clauses, Medius and Medius's Affiliates and the third party Sub-processors shall execute and adhere to Module Three (Processor to Processor) of the Standard Contractual Clauses. For Restricted Transfers from the UK that are subject to the Standard Contractual Clauses, Medius and Medius's Affiliates and the third party Sub-processors shall execute and adhere to Module Three (Processor to Processor) of the Standard Contractual Clauses in conjunction with the UK Addendum. Upon Customer's request, Medius shall make information on the transfer, and where applicable, copies of the relevant privay and security terms of Medius' agreement with the Sub-processor , without undue delay.

8.3 Medius will have the right to amend this section 8 in case Standard Contractual Clauses and/or the UK Addendum are amended, revoked or held in a court of competent jurisdiction to be invalid.

8.4 Notwithstanding section 8.2 above, for onward transfers to Sub-processors engaged prior to the effective date of this DPA, Medius may rely on the standard contractual clauses for the transfer of personal data to processors or sub-processors established in third countries as adopted by the Europe Commission under Directive 95/46/EC until 21 March 2024 with respect to transfers from the UK.

AUDIT

9.1 Medius will on a regular basis audit the security measures taken by Mediuss to protect Customer's data, including Personal Data, when providing the Services. Upon Customer's written request, Medius will provide Customer with a confidential summary of the result of such audit, for instance in the form of a SOC report, to allow for Customer to verify Medius's

compliance with Medius's security obligations set out in this DPA. The report is Medius's confidential information and is protected by the confidentiality clause set forth in the Agreement.

9.2 Customer agrees to exercise Customer's audit right by instructing Medius to execute the audit as described in secton 9.1. If Customer reasonably concludes that the provison of Medius's audit report is not sufficient to demonstrate Medius's compliance with this DPA, Medius and Medius's Affiliates shall, subject to section 9.3, make available to Customer on request all information necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits, including inspections, by Customer or an auditor mandated by Customer in relation to the Processing of Customer's Personal Data by Us. Information and audit rights of Customer only arise to the extent that the Agreement does not otherwise give Customer information and audit rights meeting the relevant requirements of Data Protection Laws and Regulations (including, where applicable, article 28(3)(h) of the GDPR).

9.3 Customer shall give Medius reasonable notice of any audit or inspection to be conducted under section 9.2 and shall make (and ensure that each of Customer's mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the audited premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. Medius does not have to give access to premises for the purposes of such an audit or inspection outside normal business hours at those premises, or for the purposes of more than one audit or inspection in any calendar year, except for any additional audits or inspections which Customer is required or requested to carry out by Data Protection Laws and Regulations or a Supervisory Authority.

9.4 Customer shall have the right, upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use by Medius of Personal Information.

LIABILITY

10.1 The parties' liability under this DPA shall be subject to the same limitation of liability as agreed between the Parties in the Agreement.

10.2 Nothing in this DPA or Agreement relieves either Party of its own direct responsibilities and liabilities under Data Protection Laws and Regulations.

11 MISCELLANEOUS

11.1 Without prejudice to the Standard Contractual Clauses' provisions of governing law and jurisdiction, the parties of this DPA hereby submits to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA.

11.2 Nothing in this DPA reduces Medius's obligations under the Agreement in relation to the protection of Personal Data or permits Medius to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses in conjunction with the UK Addendum shall prevail. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

11.3 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

_____

APPENDIX 1

1. **Subject matter of the Processing**

   The subject matter is accounts payable automation (the capture, processing and payment of invoices), supplier onboarding, procurement, contract management, and/or expense management.

2. **Data subjects**

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

   - Customer's Employees, consultants or other representatives
   - Customer's Users of the Services
   - Invoice contact persons of Customer's suppliers and other individuals referenced on invoices
   - Representatives of Customer's suppliers.
   - Individuals referenced on contracts processed for signature via the Services.
   - Customer's and Customer's contractual counterparty's signatories.

3. **Categories of data**

   Customer may submit Personal Data to Medius, the extent of which is determined an controlled by the Customer in Customer's sole discretion, and which may include but is not limited to the following categories of Personal Data:

   - First and Last name
   - Title
   - Contact information (company, email, phone, address)
   - User ID
   - Any information referenced in invoices or in contracts processed via the Services.
   - IP number
   - Bank and bank account details
   - Billing and payment data.
   - Location data (movements, GPS, GSM data etc.)
   - Identification numbers.

4. **Special categories of data (meaning sensitive personal information as defined in article 9 and 10 of the GDPR and other applicable data protection law or personal health or medical condition of an individual or the provision of health care to an individual)**

   The personal data transferred concern the following special categories of data (please specify):

   - N/A, unless defined by Customer.

5. **Processing operations**

   The personal data transferred will be subject to the following basic processing activities (please specify):

   The objective of Processing of Personal Data is to provide, maintain and develop the Services pursuant to the Agreement.

6. **Duration**

   As requested by Customer – however no longer than for the duration of the Agreement plus the period from the termination of the Agreement until deletion of Customer's data in accordance with the Agreement.

APPENDIX 2

Description of the technical and organisational security measures implemented by Medius

Medius maintains security measures appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. These measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected, taking into account the state of the art and the cost of implementation. The measures are subject to technical progress and development and Medius is therefore expressly allowed to implement adequate alternative measures as long as the general security level described in this appendix 2 is maintained.

The technical and organisational security measures that Medius currently has in place for any system that processes Personal Data with regard to prevent improper destruction, alteration, disclosure, access, and other improper forms of processing of information exported by the data exporter to the data importer, include the following areas:

- Access control
- Information Classification (and handling)
- Physical and Environmental Security
- Acceptable Use of Assets
- Clear Desk and Clear Screen
- Information Transfer
- Mobile Device and Teleworking
- Restrictions on Software Installation and Use
- Backup Routines
- Malware-protection
- Management of Technical Vulnerabilities
- Cryptographic Controls
- Communications Security
- Privacy and Protection of Personally Identifiable Information
- Subcontractor Relationship