THIS DOCUMENT IS FOR REFERENCE ONLY

The terms below no longer apply and are void and of no legal effect.
Please visit http://legal.newfold.com to access Newfold's latest terms and conditions or https://newfold.com/privacy-center for Newfold's privacy center.

If you have any questions or concerns, please contact us for further assistance.

DATA PROCESSING ADDENDUM

Last updated November 10, 2021

This Data Processing Addendum (the "**Addendum**") supplements and forms part of the Master Services Agreement, Statement of Work(s) and all other agreements governing the **Services** (collectively referred to as the "**MSA**") entered into by Newfold Digital, Inc. and/or its Affiliates ("**Buyer**" or "**Data Controller**") and **Supplier** ("**Supplier**" or "**Data Processor**"). Unless otherwise defined in this Addendum, all capitalized terms not defined in the Addendum will have the meanings given to them in the MSA.

This Addendum is put in place to ensure that Supplier, as Data Processor, Processes the Personal Data of the Buyer, as Data Controller, according to the Buyer's instructions and in compliance with Applicable Data Protection Laws.

The parties to this Addendum hereby agree to be bound by the terms and conditions as applicable with effect from 25 May 2018 or the effective date of the MSA (whichever is later) (the "**Effective Date**"). Buyer may amend this Addendum from time to time due to changes in Applicable Data Protection Laws or as otherwise determined by Buyer using commercially reasonable discretion. Any amendment will only become effective upon notification to Supplier (by email or by posting on Buyer's website) and, if Supplier does not agree to any such amendment, Supplier shall notify privacy@newfold.com.

STANDARD TERMS FOR PROCESSING ADDENDUM

1. Definitions

"**Affiliate**" means an entity that directly or indirectly controls, is controlled by, or is under common control with the Buyer. For purposes of this definition, "control" means ownership of more than fifty percent (50%) of the voting stock or equivalentownership interest in an entity.

"**Applicable Data Protection Laws**" means all data security or privacy laws and regulations applicable, which may be amended, superseded or replaced, under this Addendum, including:

i. Brazil's General Data Protection Law (LGPD)
ii. California Consumer Privacy Act (CCPA) Cal. Civ. Code 1798.100 et seq., implementing regulations
iii. Canada's Federal Personal Information Protection and Electronic Documents Act (PIPEDA)
iv. European Union's General Data Protection Regulation (GDPR), any national data protection laws made under or pursuant to the GDPR and EU e-Privacy Directive (Directive 2002/58/EC)
v. Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance

vi. UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018

"**Personal Data**" means any information relating to an identified or identifiable person or household as defined under Applicable Data Protection Laws provided by Data Controller to Data Processor for Processing on behalf of Data Controller pursuant to the MSA.

"**Consumer**" has the meaning given in the CCPA.

"**Data Subject**" means individual identified or identifiable by the Personal Data.

"**Standard Contractual Clauses**" or "**SCCs**" means the data protection clauses: i) for the transfer of Personal Data from Data Exporter to Data Importer in Third Countries without adequate level of data protection, as described in GDPR, Article 46; ii) approved by the European Commission Decision of 4 June 2021; and iii) attached to, and incorporated into, this Addendum as Schedule 1.

"**UK Standard Contractual Clauses**" means the standard data protection clauses: i) for the transfer of Personal Data from Data Exporter to Data Importer in Third Countries without adequate level of data protection, as described in Article 46 of the UK GDPR; and ii) approved by the European Commission decision 2010/87/EU.

"**Process,**" "**Processed,**" or "**Processing**" have the meaning given in the GDPR.

"**Sell**," "**Selling**," "**Sale**," or "**Sold**" have the meaning given in the CCPA.

"**Services**" means services as identified in the MSA.

"**Third Countries**" means all countries outside of the scope of the data protection laws of the European Economic Area excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time.

2.0 Conditions of Processing

2.1 This Addendum governs the terms under which Data Processor is required to Process Personal Data on behalf of Data Controller.

2.2 The Personal Data is processed solely for the purpose of providing the goods and Services described in the MSA for the duration thereof. The nature of the Processing consists of collecting, analyzing, and utilizing the data to perform the services set forth in the MSA. Personal Data that may be Processed under this MSA may belong to the following Data Subjects without limitation: (i) Buyer's customers, business partners and vendors; (ii) employees of Buyer's customers, business partners and vendors; and (iii) Buyer's employees, agents, advisors and freelancers.

2.3 In the event of any conflict or discrepancy between the terms of the MSA and this Addendum, the terms of this Addendum shall prevail, to the extent of the conflict. In the event of any conflict or discrepancy between this Addendum and any applicable UK Standard Contractual Clauses or Standard Contractual Clauses, Schedule 1, the terms of the clauses shall prevail to the extent of the conflict.

2.4 The Personal Data Processed may include, but is not limited to: (i) identification and contact information (such as name, address, title and contact details) of Buyer's customers, business partners and vendors; (ii) identification and contact information of employees of Buyer's customers, business partners and vendors; (iii) identification and contact information of Buyer's employees, agents, advisors, freelancers; and/or (iv) IT information such as IP addresses and cookies data of the Data Subjects listed in this clause.

2.5 The special categories of Personal Data Processed may include, but are not limited to: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health data, and/or sexual orientation.

3. Supplier/Data Processor's Obligations

3.1 Data Processor shall only Process Personal Data on behalf of Data Controller and in accordance with, and for the purposes set out in, the documented instructions received from Data Controller from time to time. If Data Processor cannot provide such compliance for whatever reason (including if the instruction violates Applicable Data Protection Laws), it agrees to inform Data Controller of its inability to comply as soon as reasonably practicable at the email address provided by Data Controller to Data Processor unless such law prohibits such information on important grounds of public interest.

3.2 Data Processor shall ensure that its personnel who are authorized to Process or Sell the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.3 Data Processor shall implement appropriate technical and organizational security measures, including, as appropriate those measures stipulated in Article 28 and, by extension, Article 32 of the GDPR.

3.4 Data Processor shall notify Data Controller promptly upon receipt by Data Processor of a request from a Data Subject seeking to exercise any of their rights under Applicable Data Protection Laws. Taking into account the nature of the processing, Data Processor shall, at Data Controller's expense, assist Data Controller by appropriate technical and organizational measures, for the fulfillment of Data Controller's obligation to respond to requests by Data Subjects to exercise their rights under Applicable Data Protection Laws (including the right to transparency and information, the Data Subject access right, the right to rectification and erasure, the right to the restriction of processing, the right to data portability and the right to object to processing) and any other Applicable Data Protection Laws. Data Processor shall carry out a request from Data Controller to amend or correct any of the Personal Data to the extent necessary to allow Data Controller to comply with its responsibilities under Applicable Data Protection Laws. Further, Data Processor shall carry out a request from Data Controller to block, transfer or delete any of the Personal Data to the extent necessary to allow Data Controller to comply with its responsibilities as a Data Controller.

3.5 Taking into account the nature of the Processing under the MSA and the information available to Data Processor, Data Processor shall, insofar as possible assist Data Controller in carrying out its obligations under Applicable Data Protection Laws, including Articles 32 to 36 of the GDPR, with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators. Data Processor shall promptly notify Data Controller at security@endurance.com about any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Buyers Data or any accidental or unauthorized access or any other event affecting the integrity, availability or confidentiality of Buyers Data, as required by Applicable Data Protection Laws.

3.6 Upon termination of the Processing of Personal Data by Data Processor and at the choice and expense of Data Controller, Data Processor shall either (i) delete all Personal Data; or (ii) return all Personal Data to the Data Controller and delete existing copies unless otherwise permitted or required by Applicable Data Protection Laws. To the extent any Personal Data is "deidentified" or in the "aggregate" as those terms are defined under Applicable Data Protection Laws, Data Processor may Supplier/Data

Processor such information for any commercial purpose in accordance with Applicable Data Protection Laws, including but not limited to developing analytics, and may retain, Supplier/Data Processor and disclose such information for such purpose, without restriction.

3.7 Data Controller may collect voluntary disclosures from the Data Processor or request the Data Processor to provide an expert opinion that proves compliance with their obligations under this Addendum or Applicable Data Protection Laws. Supplier shall immediately inform Buyer by emailing security@endurance.com if, in its opinion, an instruction of Data Controller infringes any Applicable Data Protection Laws. Supplier shall take all steps reasonably requested by Data Controller to ensure that the Personal Data is processed in compliance with Data Protection Laws and Regulations, including (i) any guidance on the interpretation of its provisions once it takes effect; or (ii) if changes to the membership status of a country in the European Union or the European Economic Area require modification to this Addendum, Supplier will negotiate such modifications in good faith. If Data Controller has a good faith and reasonable belief that the voluntary disclosures or the expert opinion are not reasonably sufficient to prove Data Processor's compliance with Applicable Data Protection Laws, Data Processor shall, subject to reasonable advance notice, permit the Data Controller or a third-party authorized by the Data Controller and which is not a competitor of Data Processor to carry out the audits and inspections of the processing of Personal Data by the Data Processor during normal Data Processor business hours. Data Processor may require a third-party auditor to enter into a confidentiality agreement before permitting it to carry out an audit or inspection. The auditing party shall bear its own costs in relation to such audit. The obligations set forth in this Section 3.7 shall only apply to Data Processor to the extent required by Applicable Data Protection Laws.

3.8 Data Controller acknowledges and agrees that Data Processor may, or may appoint an Affiliate or third-party subprocessor to, Process the Data Controller's Personal Data in a Third Country, provided that it ensures that such Processing takes place in accordance with the requirements of Applicable Data Protection Laws. Data Controller hereby consents to Data Processor's access to Personal Data from the United States or a Third Country to the extent necessary for Data Processor to provide the Services.

3.9 The Data Controller acknowledges and agrees that the Data Processor may process the Personal Data in the United States or Third Country in accordance with the Data Importer's obligations set out in the Applicable Data Protection Laws, the MSA and this Addendum.

3.10 Data Controller acknowledges and agrees that Data Processor relies solely on Data Controller for direction as to the extent to which Data Processor is entitled to access, use, Process and Sell Personal Data. Consequently, Data Processor is not liable for any claim brought by Data Controller or a Data Subject arising from any action or omission by Data Processor to the extent that such action or omission resulted from Data Controller's instructions.

4. Regional Specific Provisions

4.1 The Parties acknowledge and agree that some information provided to Data Processor in connection with the MSA may constitute "**Personal Information**" as defined under the CCPA. Terms defined and used under the CCPA and used in the applicable provisions of this Addendum shall be replaced as follows: "Personal Data" shall mean "Personal Information"; "Data Controller" shall mean "Business"; "Data Processor" shall mean "Service Provider"; and "Data Subject" shall mean "Consumer". Data Processor will process Personal Data in accordance with the CCPA where applicable, and solely for the purpose of providing the Services as specified in the MSA to Data Controller. Data Processor will not otherwise (i) process Personal Data for purposes other than those set forth in the MSA or as instructed by Data Controller's documented written instruction, to the extent feasible or required by CCPA; (ii) disclose

Personal Data to third parties other than Data Processor's Affiliates, for the aforementioned purposes or as required by law; (iii) sell Personal Data; or (iv) retain, use, or disclose Personal Data outside of the direct business relationship between Data Processor and Data Controller. Data Processor certifies that it understands these restrictions and will comply with them. If Data Processor must process Personal Data as otherwise required by applicable law, Data Processor shall inform Data Controller of that legal requirement before processing Personal Data, unless that law prohibits such disclosure on important grounds of public interest.

4.2 For Customer's Personal Data transferred outside of the United Kingdom for Processing, the UK Standard Contractual Clauses will apply to Personal Data transferred to any country not recognized by the United Kingdom regulatory authority as providing an adequate level of protection for Personal Data. Data Processor shall include the UK Standard Contractual Clauses, for and on behalf of Data Controller, with any relevant subcontractor agreement for services, including Affiliates.

4.3 For Customer's Personal Data transferred outside of the European Economic Area to a Third Country not recognized as by European Data Protection Authority as providing adequate level of protection for Personal Data, the Standard Contractual Clauses in Appendix 1 attached hereto as Schedule 1 shall apply. Data Processor shall include the Standard Contractual Clauses, for and on behalf of Data Controller, with any relevant subprocessor agreement for services, including Affiliates.

5. Data Controller's Obligations

5.1 Data Controller warrants that it has complied and continues to comply with the Applicable Data Protection Laws, in particular that it has obtained any necessary consents or given any necessary notices, and otherwise has a legitimate ground to disclose the Personal Data to Data Processor and enable the Processing of the Personal Data by the Data Processor as set out in this Addendum and as envisaged by the MSA.

5.2 Data Controller agrees that it will indemnify and hold harmless Data Processor on demand from and against all claims, liabilities, costs, expenses, loss or damage (including consequential losses, loss of profit and loss of reputation and all interest, penalties and legal and other professional costs and expenses) incurred by Data Processor arising directly or indirectly from a breach of this Section 5 or any Applicable Data Protection Laws.

6. Sub-Contracting

Data Controller consents to Data Processor engaging third-party subprocessors to process the Personal Data for the Permitted Purpose. Data Processor ensures that it has a written agreement in place with all subprocessors which contains obligations on the subprocessors which are no less onerous on the relevant Subcontractor than the obligations on Data Processor under this Addendum.

7. Termination

Termination of this Addendum shall be governed by the MSA.

8. Law and Jurisdiction

This Addendum and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in all respects

in accordance with the laws of the State of Florida and each of Data Controller and Data Processor hereby submits to the jurisdiction of the federal or state courts located in the County of Duval, Florida.

Schedule 1

STANDARD CONTRACTUAL CLAUSES

Module, 2, Controller to Processor

SECTION I

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 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);
   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. Not Applicable

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 the 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 its 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 organizational 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 authorized 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, under the appropriate Module, 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 defense 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 non-compliance. 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) **GENERAL WRITTEN AUTHORIZATION** The Data Importer has the Data Exporter's general authorization 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 sub-processors at least 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. 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 sub-processor 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

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 organizational 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 and as instructed by 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 authorized 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 for any damages it causes the other Party 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 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) 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 behavior 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 and practices 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 authorizing 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 organizational 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. 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, 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 PROVISIONS

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.

d) 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.

e) 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.

f) 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 of These Clauses

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. These Clauses shall be governed by the law of the Netherlands.

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 the Netherlands.

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.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):
Name: Newfold Digital, Inc. and/or Affiliate
Address: *5335 Gate Pkwy, Jacksonville, FL 32256, U.S.A.*
Contact: privacy@newfold.com

Activities relevant to the data transferred under these Clauses is identified in the MSA and other relevant agreements applicable to the Services provided to the Data Exporter by the Data Importer.
Role: Data Controller

Data importer(s):

See MSA between Data Importer and Data Exporter.

The Parties agree that execution of the Agreement by the Data Importer and the Data Exporter shall constitute execution of these Clauses by both Parties on the Effective Date of the Agreement.
Role: Data Processor

B. DESCRIPTION OF TRANSFER

Data Controller's data and Data Controller's Personal Data is transferred. Categories of Personal's Data transferred include:

i. The subject matter of the data processing covered by this Addendum is the Personal Data. The Personal Data is processed solely for the purpose of providing the goods and services described in the MSA for the duration thereof. The nature of theProcessing consists of collecting, analyzing, and utilizing the data to perform the services set forth in the MSA. Personal data that may be Processed under this MSA may belong to the following Data Subjects without limitation: (i) Buyer's customers,business partners and vendors; (ii) employees of Buyer's customers, businesspartners and vendors; and (iii) Buyer's employees, agents, advisors and freelancers.

ii. The Personal Data Processed may include, but is not limited to: (i) identification and contact information (such as name, address, title and contact details) of Buyer's customers, business partners and vendors; (ii) identification and contact information of employees of Buyer's customers, business partners and vendors; (iii) identification and contact information of Buyer's employees, agents, advisors, freelancers; and/or (iv) IT information such as IP addresses and cookies data of the Data Subjects listed in this clause.

iii. The special categories of Personal Data Processed may include, but are not limited to: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health data, and/or sexual orientation.

iv. 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer is ongoing and according to the MSA. The nature of the processing is to provide the Services requested by the Data Exporter.

C. COMPETENT SUPERVISORY AUTHORITY

Buyer and Supplier may raise a complaint with the Dutch Supervisory Authority (Autoriteit Persoonsgegevens).

Postal address
Autoriteit Persoonsgegevens
PO Box 93374
2509 AJ DEN HAAG

Telephone
Telephone number: (+31) - (0)70 - 888 85 00
Fax: (+31) - (0)70 - 888 85 01

ANNEX II

Technical and Organizational Measures to Ensure the Security of The Data

For a description of processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing see MSA.