Standard Contractual Clauses Addendum 2023
Digital Media Innovations, LLC

This Addendum sets forth the understanding between Digital Media Innovations, LLC ("Notified") and/or its applicable affiliates ("West") and the undersigned customer ("Customer") with respect to the existing Data Processing Agreement; Master Service Agreement; or similar contract as otherwise titled, as applicable, between the parties. The applicable contract is referred to herein as the "Agreement". This Addendum is effective as of the last date signed below ("Effective Date") and is incorporated into the Agreement by reference for the international transfer of personal data under the General Data Protection Regulation ("GDPR"). In the event of any conflict between this Addendum and the Agreement, the terms of this Addendum will govern. The rights and obligations contained in this Addendum will survive any assignment, transfer, conveyance, other disposition or forfeiture of rights of the Agreement. The parties agree as follows:

1. Capitalized terms, not otherwise defined herein, have the definitions set forth in the Agreement and the GDPR, as applicable.
2. As of the Effective Date, the Standard Contractual Clauses previously incorporated with the Agreement are replaced and incorporated with the Standard Contractual Clauses attached hereto in Attachment 1.1.
3. The parties ratify and confirm the Agreement in all other respects.

IN WITNESS WHEREOF, the parties hereby execute this Addendum as of the Effective Date.

CUSTOMER:

By: _____

Name: _____

Title: _____

Date: _____

DIGITAL MEDIA INNOVATIONS, LLC

By: _____

Name: _____

Title: _____

Date: _____

ATTACHMENT 1.1

STANDARD CONTRACTUAL CLAUSES-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) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

---

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(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 – Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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 organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for

attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (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 defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

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

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

(2) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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 AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least one month 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. ([3]) 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.

---

(3) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

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

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

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

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

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

Clause 14

Local laws 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 authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

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

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

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

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

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

Clause 15

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

(4) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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/ies, whether requests have been challenged and the outcome of such challenges, etc.).

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL 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.

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Sweden.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Sweden.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*

1. Name:

   Address:

   Contact person's name, position and contact details:

   Activities relevant to the data transferred under these Clauses: Use of the Services

   Signature and date:

   Role: Controller

2. ……

Data importer(s): *Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*

1. Name: Digital Media Innovations, LLC

   Address: 1350 Broadway, 25th Floor, New York, New York 10018, United States

   Contact person's name, position and contact details: Notified's Data Protection Officer is available at privacy@notified.com

   Activities relevant to the data transferred under these Clauses: Delivering the Services

   Signature and date:

   Role: Processor

2. ……

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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

- Employees, agents, advisors, customers of data exporter (who are natural persons).
- Data exporter's users authorized by data exporter to use the Services.
- Personnel, including employees, consultants, and clients of the data exporter, persons participating in events with the data exporter facilitated using the data importer's services and persons who are the subject of such events.

Categories of personal data transferred

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

- First and last name, title, position.
- Contact information (company, email, phone, physical business address)
- Personal data of employees of the data exporter stored on the data importer's system such as address, telephone number and email address.
- Billing, service and usage data of the data exporter stored on the data importer's system.

- Communication, registration, usage and log-in data.
- Personal data of users (and others, including the data subjects above) of the services in order to provision the services.

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

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis.

Nature of the processing

The data importer will process the personal data of the data exporter. The personal data of the data exporter will be retained in the data importer's databases which are physically stored within secure data centres. The data importer may, on the instruction of the data exporter, access the personal data of the data exporter. Logical access by the data importer is controlled by network and application-level access controls. The personal data of the data exporter will be stored and retained in accordance with the data importer's retention guidelines, unless the data exporter requests otherwise.

Purpose(s) of the data transfer and further processing

The processing of personal data is made for some of the following purposes to the extent it is required for the delivery of Notified's services:

- service usage.
- support, maintenance and resolution of customer queries.
- account set-up and account management.
- invoicing and collections purposes.
- records and internal administration.
- business reporting, administration and statistical analysis.
- complying with legal obligations of the data exporter and/or the data importer.
- cooperating with respect to actual or prospective legal proceedings, inquiries and investigations of governmental, judicial or regulatory authorities.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the Services or as requested otherwise by the data exporter.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

For the duration of the Services or as requested otherwise by the data exporter.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. Definitions. The following terms shall have the meanings as set forth below:
   a. "Security Incident" means the successful unauthorized access, acquisition, use, disclosure, modification, or destruction of Customer Information or interference with the operations of any of the Notified Processing Resources.
   b. "Customer Information" is the Confidential Information of Customer as such is defined in the Agreement.
   c. "Customer Information Systems" means information systems resources supplied or operated by Customer or its contractors, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, proprietary applications, printers, and internet connectivity which are owned, controlled or administered by or on behalf of Customer.
   d. "Notified Processing" means any information collection, storage or processing performed by Notified or its contractors (i) which directly or indirectly supports the services or functions now or hereafter furnished to Customer under the Agreement, (ii) using any Customer Information, or (iii) in respect of any other information if performed on behalf of Customer or in support of Customer's business, operations or services.
   e. "Notified Processing Resources" means information processing resources supplied or operated by Notified, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, printers, proprietary applications, Internet connectivity, printers and hard copies which are used, either directly or indirectly, in support of Notified Processing.
2. Security Management
   a. Notified Information Security. Notified Information Security Department exists to support both internal and external customers. In conjunction with Notified Sales and Client Engagement departments Infosec services can be invoked.
   b. Policies and Procedures. Notified shall comply with generally accepted information security management standards, like ISO27002.
   c. Infrastructure Protection. Notified shall maintain industry standard procedures to protect Notified Processing Resources, including, at a minimum:
      i. Formal security programs (policies, standards, processes, etc.);
      ii. Processes for becoming aware of, and maintaining, security patches and fixes;
      iii. Router filters, firewalls, and other mechanisms to restrict access to the Notified Processing Resources, including without limitation, all local site networks which may be accessed via the Internet (whether or not such sites transmit information);
      iv. Resources used for mobile access to Customer Information Systems shall be protected against attack and penetration through the use of firewalls; and
      v. Processes to prevent, detect, and eradicate malicious code (e.g., viruses, etc.) and to notify Customer of instances of malicious code detected on Notified Processing Resources impacting Customer Information.
3. Risk Management
   a. General Requirements. Notified shall maintain appropriate safeguards and controls and exercise due diligence to protect Customer Information and Notified Processing Resources against unauthorized access, use, and/or disclosure, considering all of the below factors. In the event of any conflict or inconsistency,

Notified shall protect the Customer Information and Notified Processing Resources in accordance with the highest applicable requirement:

i. Regulatory requirements;

ii. Information technology;

iii. Sensitivity of the data;

iv. Relative level and severity of risk of harm should the integrity, confidentiality, availability or security of the data be compromised, as determined by Notified, as part of an overall risk management program;

v. Customer's data security requirements, as set forth in this Appendix, the due diligence process and/or in the Agreement; and

vi. Any further information security requirements which are included in a statement of work or equivalent document which is attached to or relates to the Agreement

b. Security Evaluations. Notified shall periodically (no less than annually) evaluate its processes and systems to ensure continued compliance with obligations imposed by law, regulation or contract with respect to the confidentiality, integrity, availability, and security of Customer Information and Notified Processing Resources. Notified shall periodically (no less than annually) have a reputable third party perform vulnerability assessments and penetration tests of its publicly accessible Information Processing Resources. Notified shall document the results of these evaluations and any remediation activities taken in response to such evaluations.

c. Internal Records. Notified shall maintain mechanisms to capture, record, and examine information relevant to Security Incidents and other security-related events. In response to such events, Notified shall take appropriate action to address and remediate identified vulnerabilities to Customer Information and Notified Processing Resources.

d. Notified Locations. Unless previously authorized by Customer, in writing, all work performed by Notified related to the Agreement shall be performed from the Notified location(s) designated in the Agreement and/or relevant Statement of Work(s). For any location(s) outside of the 50 United States ("Offshore Locations"), where Notified performs work related to the Agreement for Customer, Notified also agrees to maintain the following security controls:

i. Notified shall conduct either a SSAE 18 Type II Audit or an ISO27001 certification at all Offshore Locations from which work is performed by Notified related to the Agreement and will provide the resulting audit reports to Customer. The audits or certifications will be conducted once annually, and each report will cover a twelve-month term. The audit report will be issued to Customer within 30 days upon request.

ii. Notified will comply with all future SSAE versions, ISO27001 standards, or that of its successor(s), as issued by the SEC and the Public Company Accounting Oversight Board, or International Standards Organization (ISO).

4. Personnel Security

a. Access to Customer Information. Notified shall require its employees, contractors and agents who have, or may be expected to have, access to Customer Information or Customer Information Systems to comply with the provisions of the Agreement, including this Appendix and any other applicable agreements binding upon Notified. Notified will remain responsible for any breach of this Appendix by its employees, contractors, and agents.

b. Security Awareness. Notified shall ensure that its employees and contractors remain aware of industry standard security practices, and their responsibilities for protecting the Customer Information. This shall include, but not be limited to:

i. Protection against malicious software (such as viruses);

ii. Appropriate password protection and password management practices; and

iii. Appropriate use of workstations and computer system accounts.

iv. Notified requires annual Information Security and Compliance training, Privacy training and Business Ethics Training for all employees and contract resources

c. Sanction Policy. Notified shall maintain a sanction policy to address violations of Notified's internal security requirements or security requirements which are imposed on Notified by law, regulation, or contract.

d. Supervision of Workforce. Notified shall maintain processes for authorizing and supervising its employees, temporary employees, and independent contractors and for monitoring access to Customer Information, Customer Information Systems and/or Notified Processing Resources.

e. Background Checks. Notified shall maintain processes to determine whether a prospective member of Notified's workforce is sufficiently trustworthy to work in an environment which contains Notified Processing Resources and Customer Information and/or access to Customer Information Systems. Such background checks, when applicable, may have been performed as part of Notified's standard pre-employment screening process and include the following, when applicable, at a minimum: (i) Social Security Verification (confirms applicant's date of birth, Social Security number, and former addresses, (ii) Federal Watch Lists (no applicant will be considered for employment if they appear on a Federal Watch List; including but not limited to OFAC's Specially Designated Nationals List, FDA's Debarment list, Registered Sex Offender list, OIG's Exclusion List, OCC's Enforcement Actions list, and (iii) Criminal History check of at least 7 years (more where contractually required),. Dependent upon employee role, credit checks are required for employees working with money or clients' financial data, and for roles at or above Director level.

5. Physical Security. Notified shall maintain appropriate physical security controls (including facility and environmental controls) to prevent unauthorized physical access to Notified Processing Resources and areas in which Customer Information is stored or processed. Where practicable, this obligation shall include controls to physically protect hardware (e.g., lockdown devices). Notified shall adopt and implement a written facility security plan which documents such controls and the policies and procedures through which such controls will be maintained. Notified shall maintain appropriate records of maintenance performed on Notified Processing Resources and on the physical control mechanisms used to secure Notified Processing Resources.

6. Site Outage. Notified Sales or Client Engagement teams shall promptly report to Customer any Notified site outages where such outage may impact Customer or Notified's ability to fulfill its obligations to Customer.

7. Communication Security

a. Exchange of Customer Information. The parties agree to utilize a secure method of transmission when exchanging Customer Information electronically.

b. Encryption. Notified shall maintain encryption, in accordance with standards mutually agreed upon between the parties, for all transmission of Customer Information via public networks (e.g., the Internet). Such transmissions include, but are not limited to:

i. Sessions between web browsers and web servers;

ii. Email containing Customer Information (including passwords); and

iii. Transfer of files via the Internet (e.g., SFTP).

c. Protection of Storage Media. Notified shall ensure that storage media containing Customer Information is properly sanitized of all Customer Information in accordance with DOD5220.22-M (minimum 3-pass wipe) or is destroyed in accordance with applicable laws and regulations prior to disposal or re-use for non-Notified Processing. All media on which Customer Information is stored shall be protected against unauthorized access or modification. Notified shall maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal and transfer of storage media used for Notified Processing or on which Customer Information has been stored.

d. Data Integrity. Notified shall maintain processes to prevent unauthorized or inappropriate modification of Customer Information, for both data in transit and data at rest.

8. Access Control

a. Identification and Authentication. All access to any Customer Information or any Notified Processing Resources shall be Identified and Authenticated as defined in this Section. "Identification" refers to processes which establish the identity of the person or entity requesting access to Customer Information

and/or Notified Processing Resources. "Authentication" refers to processes which validate the purported identity of the requestor. For access to Customer Information or Notified Processing Resources, Notified shall require Authentication by the use of an individual, unique user ID and an individual password and/or other appropriate Authentication technique (e.g. soft token, pin, etc.). Notified shall obtain written approval from Customer prior to using digital certificates as part of Notified's Identification or Authorization processes. Notified shall maintain procedures to ensure the protection, integrity, and soundness of all passwords created by Notified and/or used by Notified in connection with the Agreement.

b. Account Administration. Notified shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for Notified Processing Resources and Customer Information. These processes shall be required for both Customer-related accounts and Notified's internal accounts for Notified Processing Resources and shall include procedures for granting and revoking emergency access to Notified Processing Resources and Customer Information. All access by Notified's employees or contractors to Customer Information Systems shall be subject to advance approval by Customer and shall follow Customer standard policies and procedures.

c. Access Control. Notified shall maintain appropriate access control mechanisms to prevent all access to Customer Information and/or Notified Processing Resources, except by (i) specified users expressly authorized by Customer and (ii) Notified personnel who have a "need to access" to perform a particular function in support of Notified Processing. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions.

9. Network Security Authorized Access. Notified shall only have access to Customer Information Systems authorized by Customer and shall use such access solely for providing services to Customer. Notified shall not attempt to access any applications, systems or data which Notified does not need to access in order to perform services for Customer. Notified further agrees to access such applications, data and systems solely to the extent minimally necessary to provide services to Customer.

10. Business Continuity Management. Notified will, establish and maintain (i) business continuity and disaster recovery plans ("Contingency Plans") for critical functions, technology and systems in support of the Services herein to enable recovery of said Services within the agreed upon Recovery Time and Recovery Point objectives in the event of a disaster or other unexpected disruption in Services. (ii) Notified will review, update and exercise the operability of applicable Contingency Plans in support of the Services herein by conducting recovery exercises of Contingency Plans at least annually, per Notified business continuity policy.

11. Compliance with Laws. Notified shall comply with all applicable laws, regulations, ordinances and requirements relating to the confidentiality, integrity, availability, or security of Customer Information applicable to Notified in performing its obligations under the Agreement.

12. Third Parties. Notified shall ensure that any agent, including a subcontractor, to whom Notified provides Customer Information agrees to maintain reasonable and appropriate safeguards to protect such Customer Information; provided, however, that Notified shall not assign, delegate, or subcontract any obligation of Notified owed to Customer in violation of the Agreement.

13. Amendments. This Appendix may be modified by a written agreement executed by Notified and Customer. Notwithstanding the foregoing or anything else, Notified may amend this Appendix by providing thirty (30) days advance written notice of such amendment if Notified reasonably determines that such amendment is necessary for Notified to comply with any federal, state or local law, regulation, ordinance, or requirement relating to the confidentiality, integrity, availability, or security of individually identifiable medical or personal information.