DATA PROCESSING ADDENDUM

1. Definitions

1.1 For the purposes of this Addendum, the following terms are defined unless the context otherwise requires:

"**Data Subject**", "**Process**", "**Processed**" or "**Processing**" shall each have the meaning as set out in the Data Protection Legislation.
"**Controller to Processor Clauses**" means, as relevant, the standard contractual clauses for the transfer of Personal Data to data processors established in third countries set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (for Module 2), or any equivalent clauses issued by the relevant competent authority of the UK in respect of transfers of Personal Data from the UK, in each case as amended, updated or replaced from time to time.
"**Regulator**" means the data protection supervisory authority which has jurisdiction over a Data Controller's Processing of Personal Data.
"**Third Countries**" means (i) in relation to Personal Data transfers from the EEA, any country outside of the scope of the data protection laws of the EEA, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; and (ii) in relation to Personal Data transfers from the UK, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time.
"**UK Addendum**" means the UK international data transfer addendum to the standard contractual clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, approved by the UK Information Commissioner's Office under section 119A of the DPA, and set out in Annex I to this Exhibit D.

2. Background

2.1 The Parties shall comply with the Data Protection Legislation as it applies to Personal Data processed under this Agreement. For the avoidance of doubt, Exhibit D is in addition to, and does not relieve, remove, or replace, each Party's obligations under any Data Protection Legislation.

2.2 The Client or the Client's Affiliate (each being a "**Data Controller**") wishes to appoint Tigunia (the "**Data Processor**") to Process Personal Data, as further described in Part B (Processing Details).

3. **Data Processor's Obligations**

3.1 Subject to the terms of the Controller to Processor Clauses (see paragraphs 4 and 4.1 below), to the extent the Data Processor Processes Personal Data on behalf of the Data Controller, it shall:

(a) Process the Personal Data only on documented instructions from the Data Controller, including (where applicable) with regard to transfers of Personal Data to Third Countries or an international organization, unless required to Process such Personal Data by an applicable law to which the Data Processor is subject; in such a case, the Data Processor shall inform the Data Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

(b) ensure that its personnel authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) implement and hold in force for the term of this Agreement specific technical and organizational security measures as required by the Data Protection Legislation and Part C (Technical and organizational measures including technical and organizational measures to ensure the security of the data);

(d) taking into account the nature of the Processing, assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in the Data Protection Legislation;

(e) notify the Data Controller without undue delay, and in any event within forty-eight (48) hours about any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data belonging to the Data Controller(s) or any accidental or unauthorized access or any other event affecting the integrity, availability or confidentiality of the Personal Data belonging to the Data Controller(s) (including a Personal Data Breach, as defined in Data Protection Legislation), and work together with the Data Controller in good faith to mitigate any adverse effects for such breach;

(f) taking into account the nature of the Processing and the information available to the Data Processor, assist the Data Controller (at Data Controller's expense) in ensuring compliance with the Data Controller's obligations under the Data Protection Legislation, including to: (i) implement appropriate technical and organizational security measures; (ii) notify Personal Data breaches to Regulators and/or individuals; and (iii) conduct data protection impact assessments; and (iv) prior consultation with Regulators, in each case as required by any Data Protection Legislation;

(g) maintain and make available to the Data Controller records and information to demonstrate its compliance with the obligations laid down in this paragraph 3 and under the Data Protection Legislation, and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller;

(h) shall promptly inform the Data Controller if, in its opinion, an instruction of the Data Controller infringes the Data Protection Legislation; and

(i) at the request of the Data Controller, delete or return all of the Personal Data to the Data Controller after the end of the provision of Services relating to Processing, and delete existing copies unless the Data Processor is required to store such Personal Data under applicable law.

4. **International Transfers**

4.1 Where the Data Controller is established in the UK or an EEA member state, then the Data Processor may process data in, or transfer Personal Data to an Affiliate in, a Third Country; provided that the Data Processor (or such Affiliate which will be processing the Personal Data in such Third Country) complies with the data importer's obligations set out in the Controller to Processor Clauses which are hereby incorporated into and form part of this Agreement by reference (and Part A (List of Parties) shall apply for the purposes of Annex I.A to the Controller to Processor Clauses, Part B (Processing Details) shall apply for the purposes of Annex I.B to the Controller to Processor Clauses and Part C (Technical and Organizational Security Measures) shall apply for the purposes of Annex II to the Controller to Processor Clauses), which shall incorporate the UK Addendum where the Data Controller is established in the UK. The Data Controller shall comply with the data exporter's obligations set out in the Controller to Processor Clauses, which shall incorporate the UK Addendum where the Data Controller is established in the UK.

4.2 At the commencement of this Agreement, the data exporter shall be Tigunia's applicalble client, and the Parties agree that the Controller to Processor Clauses shall incorporate the UK Addendum as per Annex I to this Exhibit D.

4.3 The Parties shall update Part A (List of Parties) as applicable where the data exporter is another Affiliate of the Client.

4.4 Where the Data Controller is an Affiliate of Client based in the EEA, then for the purposes of the Controller to Processor Clauses used in relation to any data exports from that Affiliate to data importer:

(a) clause 7 (*Docking clause*) shall apply;

(b) in clause 9(a) (*Use of sub-processors*), the data importer / Data Processor has the data exporter's / Data Controller's general authorization for the engagement of sub-processors(s). The data importer / Data Processor shall specifically inform the data exporter / Data Controller in writing of any intended changes to that list

through the addition or replacement of subprocessors at least thirty (30) days in advance;

(c) in clause 11 (*Redress*), the relevant data importer does not agree to offer the optional redress mechanism to data subjects;

(d) in clause 13(a) (*Supervision*), as applicable;

(e) in clause 17 (*Governing law*), the governing law shall be in accordance with Option 2 and the parties specify the laws of Ireland as the relevant EU Member State; and

(f) in clause 18(b) (*Choice of forum and jurisdiction*), the Irish courts will apply as the relevant EU Member State.

For the avoidance of doubt, the Parties acknowledge that nothing in this paragraph creates any substantive amendments to the Controller to Processor Clauses.

4.5 As part of the Data Controller's assessment of the adequacy of the protection of the Personal Data in accordance with the requirements of applicable law, including taking into account the legal regime of the jurisdiction of the Data Processor (and in collaboration with the Data Processor as necessary), where applicable, the Data Controller has identified additional safeguards as further described in paragraph 4.6.

4.6 Additional safeguards required to be put in place to ensure the adequate protection of the Personal Data transferred, include, among other measures:

(a) secure encryption of the personal data in transit and at rest;

(b) technical measures to secure relevant encryption keys;

(c) secure pseudonymization of the personal data;

(d) technical measures to secure the additional information which allows pseudonymized data to be attributed to a specific data subject.

4.7 The Data Processor agrees and warrants:

(a) without prejudice to Clause 14(f) of the Controller to Processor Clauses, that, in the event the Controller to Processor Clauses ceases to be an appropriate safeguard for the transfer of Personal Data, in accordance with applicable law or by virtue of a binding decision by a competent supervisory authority, the Data Controller shall be entitled to suspend the transfer of Personal Data;

(b) that any information provided by it or at its direction to the Data Controller for the purposes of the Data Controller's assessment of the adequacy of the protection of the Personal Data pursuant to this paragraph 4.7 was, when provided, accurate, and complete;

(c) to assist the Data Controller with the Data Controller's continuing assessment of the adequacy of the protection of the Personal Data in accordance with the requirements of applicable law and pursuant to Clause 14 of the Controller to Processor Clauses; and

(d) that, in the event the data transfer and data processing activities are suspended or terminated pursuant to the Controller to Processor Clauses, to the extent permitted by the Data Protection Legislation, its cessation of the data processing

activities will not be prevented by, or be in breach of, and will not give rise to any third party rights or remedies pursuant to, any binding obligation on the data importer under the Controller to Processor Clauses or any other agreement between the Data Processor and the Data Controller (or any of its Affiliates) in relation to the Personal Data and data Processing activities.

4.8 Upon receipt of any legally binding order or request for disclosure of the Personal Data by a law enforcement authority or other competent public or government authority, the Data Processor will:

(a) if permitted by applicable laws and the Data Protection Legislation, use reasonable efforts to re-direct the relevant authority to request or obtain the Personal Data directly from the Data Controller;

(b) in addition to promptly notifying the Data Controller (and where possible, the data subject) of the request or order pursuant to clause 15.1(a) of the Controller to Processor Clauses, use reasonable efforts to assist the Data Controller in its efforts to oppose the request or order, if applicable;

(c) in the event it is prohibited by applicable laws from notifying the Data Controller and/or the data subject of the request or order, use best efforts to obtain a waiver of the prohibition as soon as possible pursuant to clause 15.1(b) of the Controller to Processor Clauses, and challenge such request or order in a court of competent jurisdiction and seek relevant permission to allow the Data Controller to intervene in the proceedings; and

(d) in the event such request or any subsequent disclosure or other action by the Data Processor prevents or would prevent the Data Processor from complying with the Controller to Processor Clauses or the instructions of the Data Controller, the Data Processor agrees, pursuant to clause 14(e) and clause 16 of the Controller to Processor Clauses, to promptly inform the Data Controller of its inability to comply.

5. Sub-Processing

5.1 The Data Controller hereby grants the Data Processor general written authorization to engage all sub-processors used by Tigunia and to use, add or replace sub-processors provided that the Data Processor shall inform the Data Controller in writing at least thirty (30) days in advance. The Data Controller will have seven (7) days from the date of receipt of the notice to approve or reject the change. In the event of no response from the Data Controller, the sub-processor will be deemed accepted.

5.2 Tigunia will provide to the Client its list of sub-processors that it will use in the delivery of the Services upon Client's request.

5.3 In the event that the Data Processor engages a sub-processor for carrying out specific Processing activities on behalf of the Data Controller, the same data protection obligations imposed on the Data Processor as set out in this Exhibit D shall be imposed

on the sub-processor, in particular ensuring that the sub-processor provides sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the Data Protection Legislation. Where the sub-processor fails to fulfil its obligations, the Data Processor shall remain fully liable under the Data Protection Legislation to the Data Controller for the performance of the sub-processor's obligations.

6. **Changes in Data Protection Legislation**

The parties agree to negotiate in good faith modifications to this Exhibit D if changes are required for the Data Processor to continue to process the Personal Data as contemplated by this Agreement in compliance with the Data Protection Legislation or to address the legal interpretation of the Data Protection Legislation, including: (i) to comply with the GDPR or any national legislation implementing it, or the UK GDPR or the DPA, and any guidance on the interpretation of any of their respective provisions; (ii) the Controller to Processor Clauses or any other mechanisms or findings of adequacy are invalidated or amended, or (iii) if changes to the membership status of a country in the European Union or the European Economic Area require such modification.

Part A - List of Parties

Data Exporter

Country:	As applicable
Name:	Tigunia's Client
Address:	As applicable
Contact person's name, position and contact details:	As applicable
Activities relevant to the data transferred under the Controller to Processor Clauses:	See Part B (*Processing Details*)

Role (controller/processor):	Controller

Data Importer

Country:	United States
Name:	Tigunia, LLC
Address:	P.O. Box 31014, Edmond, OK 73003, and is registered in the State of Colorado
Contact person's name, position and contact details:	As per notice details in Agreement
Activities relevant to the data transferred under the Controller to Processor Clauses:	See Part B (*Processing Details*)
Role (controller/processor):	Processor

Part B - Processing Details Categories of data subjects whose Personal Data is transferred

The Personal Data to be Processed concerns the following categories of data, each to the extent required in relation to the relevant service provision:

- Employees, officers, directors, contractors, consultants, representatives, agents of Data Controller and Data Controller's affiliates.
- Client's customers and suppliers.

Categories of Personal Data transferred

The Personal Data to be Processed concerns the following categories of data, each to the extent required in relation to the relevant service provision:

- As determined by the Client

Name and contact details including email addresses:

- As determined by the Client

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.

- Not applicable.

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

- The Personal Data will be Processed for the Term of the Client's Master Services Agreement.

Nature of the Processing

- As determined by the Client

Purpose(s) of the data transfer(s) and further processing

- Provision of the Services pursuant to each Statement of Work entered into under the Master Services Agreement.

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

- The above categories of Personal Data will not be stored for longer than necessary for the legally permissible purpose(s) for which they were collected and as required under applicable retention policies and/or in accordance with the Data Protection Legislation.

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

- Transfers to sub-processor(s) (if any) will be conducted in accordance with the terms of this Agreement.

Part C - Technical and organizational measures

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Tigunia shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk consistent with its obligations under the Security Standards.

ANNEX I – UK ADDENDUM

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The effective date of this Agreement.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Client	Tigunia, LLC; P.O. Box 31014, Edmond, OK 73003, and is registered in the State of Colorado
Key Contact	Data Protection Officer	James Nicholas, V.P., Information Technology

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Controller to Processor Clauses (Module 2) Date: the effective date of this Agreement.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Part 1, Table 1

Annex 1B: Description of Transfer: See Part B of Exhibit D

Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: See Part C of Exhibit D.

Annex III: List of Sub processors: As per paragraph 5 of Exhibit D

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: • Neither Party

Part 2: Mandatory Clauses

1. Entering into this Addendum
   (a) Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
   (b) Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

2. Interpretation of this Addendum
   (a) Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.

UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to
	time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

(b) This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

(c) If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

(d) If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

(e) If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

(f) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this Addendum has been entered into.

3. Hierarchy

(a) Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

(b) Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or

conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

(c) Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

4. Incorporation of and changes to the EU SCCs

(a) This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

(i) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

(ii) Sections 9 to 11 override Clause 5 (*Hierarchy*) of the Addendum EU SCCs; and

(iii) this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

(b) Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

(c) No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

(d) The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

(i) References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

(ii) In Clause 2, delete the words: "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";

(e) Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

(f) Clause 8.8(i) of Module 2 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

(g) References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

(h) References to Regulation (EU) 2018/1725 are removed;

(i) References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

(j) Clause 13(a) and Part C of Annex I are not used;

(k) The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”; (l) In Clause 16(e), subsection (i) is replaced with:
“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

(m) Clause 17 is replaced with:
“These Clauses are governed by the laws of England and Wales.”; (n)
Clause 18 is replaced with:
“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

(o) The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

5. Amendments to this Addendum

(a) If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

(b) From time to time, the ICO may issue a revised Approved Addendum which:

(i) makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

(ii) reflects changes to UK Data Protection Laws;

(iii) The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

(c) If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

(i) its direct costs of performing its obligations under the Addendum; and/or

(ii) its risk under the Addendum, and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

(d) The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.