GRUNTWORK DATA PROCESSING AGREEMENT

This DATA PROCESSING ADDENDUM (the "**Addendum**") is between Gruntwork, Inc. (the "**Data Processor**") and Data Controller (as defined below) (collectively the "**Parties**") and supplements the Gruntwork Customer Agreement, or other agreement between Customer and Gruntwork governing Customer's use of the Services (the "**Agreement**") when the GDPR applies to your use of the Service to process Customer Data. This Addendum is an agreement between you and the entity you represent ("**Customer**", "**you**", or "**your**") and Gruntwork, Inc. ("**Gruntwork**"). Unless otherwise defined in this Addendum or in the Agreement, all capitalized terms used in this Addendum will have the meanings given to them in Section 1 of this Addendum.

1. Definitions

1.1 For the purposes of this Addendum, the following expressions have the following meanings unless the context otherwise requires:

"**Applicable Data Protection Laws**" means GDPR and Directive 2002/58/EC and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including, where applicable, the Data Protection Act 2018), other data protection laws of the EU, its Member States, Switzerland, Iceland, Liechtenstein and Norway and the United Kingdom, applicable to the Processing of Personal Data under the Customer Agreement and this Addendum, including: United Kingdom General Data Protection Regulation and the UK Data Protection Act 2018 (collectively "UK GDPR") and all other applicable laws relating to processing of personal data and privacy that may exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by supervisory authorities;

"**Client Personal Data**" means Personal Data provided by Data Controller to Data Processor for Processing on behalf of Data Controller pursuant to the Customer Agreement which is subject to the Applicable Data Protection Laws;

"**Controller-to-Processor Clauses" or "Model Clauses"** means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and attached hereto.

"**Data Subject**", "**Personal Data**", "**Process**", "**Processed**" or "**Processing**" have the meaning given in the GDPR and includes equivalent terms under Applicable Data Protection Laws;

"**GDPR**" means to the extent applicable to the processing activities: (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and (ii) the UK GDPR;

"Security Incident" means a breach of Data Processor's security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Personal Data; and

"**Third Country**" means, in each case to the extent applicable to the processing activities all countries other than those countries in respect of which an adequacy finding has been granted under Applicable Data Protection Laws.

2. Conditions of Processing

2.1 This Addendum governs the terms under which Data Processor is required to Process Client Personal Data on behalf of Data Controller. In the event of any conflict or discrepancy between the terms of the Customer Agreement and this Addendum, the terms of this Addendum prevail to the extent of the conflict.

2.2 The Parties agree that this Addendum replaces and supersedes any existing data processing addendum, attachment, exhibit or Model Clauses that the Parties may have previously entered into in connection with the Services.

3. Details of Data Processing

3.1 **Subject Matter:** The subject matter of the data processing under this Addendum is Client Personal Data.

3.2 **Duration:** The duration of the data processing under this Addendum is determined by the Data Controller.

3.3 **Purpose:** The purpose of the data processing under this Addendum is the provision of Services initiated by Data Controller from time to time.

3.4 **Nature of the Processing:** Computation, storage, reference and such other Services as described in the Agreement and initiated by Data Controller from time to time.

3.5 **Type of Customer Data:** Client Personal Data.

3.6 **Categories of data subjects:** The data subjects could include Data Processor's customers, customer employees, and customer contractors.

4. Data Processor's Obligations

4.1 Data Controller Instructions. Data Processor shall only Process Client 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, which are set out in the Customer Agreement and relevant Work Order or Statement of Work, if applicable. Notwithstanding the foregoing, Data Processor may Process Client Personal Data as required under applicable law, such as to comply with requests by public authorities. In this situation, Data Processor will take reasonable steps to inform Data Controller of such a requirement before Data Processor Processes the data, unless the law prohibits this.

4.2 Confidentiality. Data Processor ensures that its personnel who are authorized to Process the Client Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.3 Security. The Data Processor shall implement appropriate technical and organizational measures designed to protect against unauthorized or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Client Personal Data. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction, damage or theft of the Client Personal Data and having regard to the nature of the Client Personal Data which is to be protected and shall be as set forth in accordance with the Data Processor's then current Data and Information Security Program ("Program") located at https://gruntwork.io/information-security-policy. The Data Controller acknowledge that Data Processor may change the security measures through the adoption of new or enhanced security technologies and authorises Data Processor to make such changes provided that they do not materially diminish the level of protection.

4.4 Security Incidents. Taking into account the nature of the Processing and the information available to Data Processor, Data Processor shall insofar as possible and at Data Controller's expense, assist Data Controller in Data Controller's obligation to notify a supervisory authority or data subjects (as applicable) about a Security Incident. Data Processor shall cooperate with and assist Data Controller by including in the notification such information about the Security Incident as Data Processor is able to disclose to Data Controller, taking into account the nature of the Processing, information available to Data Processor, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Data Controller agrees that it is best able to determine the likely consequences of a Security Incident. Data Processor will promptly notify Data Controller about a Security Incident without undue delay after becoming aware of the Security Incident, and take mitigation measures to address the Security Incident.

4.5 Deletion / return of Client Personal Data

Subject to the Customer Agreement, within a reasonable period time following receipt of written notice from Data Controller, Data Processor shall delete or return to the Data Controller Client Personal Data after the end of the provision of the Services, unless applicable law requires storage of the Client Personal Data. To the extent Data Processor maintains Client Personal Data on back-ups, such back-ups shall be deleted pursuant to the Data Processor's standard operating procedure.

4.6 Data Subject Requests. Taking into account the nature of the Processing, Data Processor shall, insofar as possible, and at Data Controller's expense, assist Data Controller by appropriate technical and organizational measures, for the fulfilment of Data Controller's obligation to respond to requests by Data Subjects to exercise their rights under the Applicable Data Protection Law. Data Processor, insofar as possible and to the extent Data Controller in its use of the Services, does not have the ability to address a Data Subject request, shall assist Data Controller to amend, correct,

block, transfer or delete any of the Client Personal Data to the extent necessary to allow Data Controller to comply with its responsibilities as a data controller.

4.7 Audits and Reports. Data Processor shall assist the Data Controller with audits to the extent provided for in this Section 4.7:

4.7.1 Data Processor uses external auditors to verify the adequacy of its security measures. This audit will be performed annually according to applicable industry standards by independent third-party security professionals at Data Processor's selection and expense and will result in the generation of an audit report ("Report"), which will be Data Processor's Confidential Information. At Data Controller's written request, and provided that the Parties have a special-purpose non-disclosure agreement in place, Data Processor will provide those named employee(s) of Data Controller on a need-to-know basis with a copy of the Report so that such individuals can reasonably verify for Data Controller Data Processor's compliance with its privacy and security obligations under this Addendum and Applicable Data Protection Laws.

4.7.2 If Data Controller reasonably considers that the Report fails to verify Data Processor's compliance with the security obligations under the Addendum or to demonstrate compliance with Applicable Data Protection Laws, then Data Controller must notify Data Processor in writing within ten (10) days of receipt of the Report. Such notice shall list which provisions of the GDPR the Report fails to demonstrate compliance. Data Controller's failure to notify Data Processor within such 10-day period shall be deemed Data Controller's acceptance of the Report as full satisfaction of Data Processor's obligations under the Addendum and Data Controller's rights under the Applicable Data Protection Laws. Upon receipt of Data Controller's notice, Data Processor shall arrange for Data Controller to meet with Data Processor within ten (10) days to review and discuss Data Controller's concerns with the Report as set forth in the notice. If Data Controller's issues are not resolved within thirty (30) days of such a meeting, then Data Controller may request an audit as set forth herein.

4.7.3 If Data Processor accepts such request, Data Processor shall permit Data Controller to appoint an independent, accredited third-party auditor which is not a competitor of Data Processor, to carry out, no more frequently than once a calendar year, an audit of the processing of Client Personal Data by Data Processor, on thirty (30) days' advance notice during Data Processor's regular business hours. Data Controller shall require such third-party auditor to enter into a confidentiality agreement before permitting it to carry out the audit. Data Controller agrees that persons carrying out the audit under this Section 4.7 shall be accompanied by representatives of Data Processor. Data Controller's third-party auditor shall only have a right to audit or inspect Data Processor premises or parts thereof which are used for the Processing of Client Personal Data. Data Controller is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Data Processor expends for any such audit, in addition to the rates for services performed by Data Processor.

4.7.4 Data Controller agrees that the audits described in the Model Clauses shall be carried out solely in accordance with this Section 4.7. If the Model Clauses apply, nothing in this Section 4.7 varies or modifies the Model Clauses nor affects any supervisory authority's or data subject's rights under the Model Clauses.

4.8 Data Storage. Data Processor shall store the Client Personal Data, at rest, within the following geographic areas as requested by Data Controller:

4.8.1 Client Personal Data is stored in the EEA, Switzerland or the United Kingdom for all Clients located within the EEA, Switzerland or the United Kingdom and for Clients located outside of those territories, such Client Personal Data is stored in North America. Client Personal Data sent to Data Processor's affiliate based in India for the purposes of providing customer support and services is stored in India.

4.9 Data Transfers. Data Controller acknowledges and agrees that Data Processor may, or may appoint an affiliate or third party subprocessor to transfer the Client Personal Data to a Third Country, provided that it ensures that such transfer takes place in accordance with the requirements of Applicable Data Protection Laws. Upon request, Data Processor shall provide Data Controller with a list of the locations to which it has transferred the data.

4.10 Where the Data Processor transfers Client Personal Data to any Third Country, Data Processor shall comply with the data importer's obligations set out in the Model Clauses, which are attached hereto. These Model Clauses are hereby incorporated into and form part of this Addendum. For the avoidance of doubt, Data Controller shall comply with the data exporter's obligations set out in the Model Clauses. Data Controller hereby grants Data Processor a mandate to

execute the Model Clauses, for and on behalf of Data Controller, with any relevant subcontractor (including affiliates) it appoints. Where the Model Clauses apply, the Data Controller acknowledges the following:

4.10.1 *Instructions.* For the purposes of the Model Clauses, processing in accordance with this Addendum and the Customer Agreement, or as provided in writing by Data Controller from time to time (subject to the Data Processor's right to charge additional sums at its current rates should the scope of the agreed services be exceeded), is deemed to be an instruction by Data Controller to process Client Personal Data;

4.10.2 *Sub-Processors.* Pursuant to the Model Clauses the Data Controller acknowledges that the Data Processor may engage third-party Sub-processors in connection with the provision of the Services and that the Data Processor shall make available to the Data Controller the current list of all Sub-processors as set out in Section 6 below. The Data Processor will notify the Data Controller of any new Sub-processors engaged by the data importer as set out in Section 6 below.

4.10.3 *Copies of Sub-Processor Agreements*. The Data Controller agree that copies of any Sub-processor agreements that must be provided pursuant to the Model Clauses may have all commercial information or clauses unrelated to the Model Clauses or their equivalent removed by the Data Processor beforehand; and that such copies will be provided by the Data Processor in a manner to be determined in its discretion, only upon written request by the Data Controller.

4.11 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 and Process Client 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.

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 data to Data Processor and enable the Processing of the Client Personal Data by the Data Processor as set out in this Addendum and as envisaged by the Customer Agreement.

5.2 The Data Controller warrants that the instructions that the Data Controller provides to the Data Processor in relation to the processing of Client Personal Data complies with Applicable Data Protection Law.

6. Sub-Processors

6.1 Data Controller provides Data Processor with consent to the use by Data Processor of the following Sub-processors to carry out Processing of the Client Personal Data, in each case based in the jurisdictions set out at Section 4.8.1, for the purposes of providing solutions to Data Processor: https://gruntwork.io/legal/subprocessors.

6.2 If Data Processor appoints a new Sub-processor to Process Client Personal Data, Data Processor shall update the link above and provide Data Controller with twenty business days' prior written notice, during which time Data Controller can object in writing to the appointment. If Data Controller does not object, Data Processor may proceed with the appointment. If Data Controller provides Data Processor with a timely objection and such objection is based on reasonable grounds relating to data protection, then the Parties shall engage in a good-faith discussion of such objection. If it can be reasonably demonstrated by the Data Controller that the new Sub-processor is unable to Process Client Personal Data in compliance with the terms of this Addendum and Data Processor cannot provide an alternative Sub-processor, or the Parties are not otherwise able to achieve resolution, Data Processor shall, in its sole discretion, either: (i) comply with such objection and not proceed with the appointment in respect of Data Controller; or (ii) proceed with the appointment and, as Data Processor's sole liability and Data Controller's sole and exclusive remedy, terminate the Agreement, or part thereof, which is affected by such change on written notice to Data Controller. Data Processor ensures that it has a written agreement in place with all Sub-processors which contains obligations on the Sub-processor which are no less onerous on the relevant Sub-processor than the obligations on Data Processor under this Addendum, save that the Data Processor is excepted from agreeing provisions equivalent to Section 4.7.

7. Limitation of Liability

7.1 Notwithstanding anything to the contrary set forth in this Addendum, Data Processor's total liability to the Data Controller, whether in contract, tort, negligence, strict liability or by statute or otherwise, arising out of or relating to this Addendum, shall not exceed the annual fees payable by Data Controller to the Data Processor in the 12 months preceding the date on which the cause of action arose. All liability is cumulative and not per incident. This limitation will apply notwithstanding any failure of essential purpose of any limited remedy

provided herein. The foregoing limitation of liability does not limit either Party's liability for any cause of action for death, bodily injury, or tangible damage to property of either party.

8. Variations

8.1. This Addendum may be updated from time to time by the Data Processor in its absolute and sole discretion with any such updated version posted at https://gruntwork.io/legal/dpa, or on any successor website, provided, however, that no such update shall materially diminish the privacy or security of Client Personal Data.

9. Law and Jurisdiction

9.1. 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 is governed by and construed in all respects in accordance with the laws of the State of Delaware and each party hereby submits to the exclusive jurisdiction of the courts of Delaware.

IN WITNESS WHEREOF, the Parties acknowledge their agreement to the foregoing by due execution of the DPA by their respective authorized representatives.

CUSTOMER

Signature: _____

Customer Legal Name: _____

Print Name: _____

Title: _____

Date: _____

DPO/Contact for data protection enquiries:

_____

GRUNTWORK, INC.

Signature:

Print Name: Josh Padnick

Title: Director

Date: August 24, 2023

DPO/Contact for data protection enquiries: Privacy Team, privacy@gruntwork.io

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)[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 8.1(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); and

(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

Docking clause

[Intentionally left blank]

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 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 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;

[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.

(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.

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) 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 10 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.[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.

Clause 10

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

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

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

[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.

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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Iceland.

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 Iceland.

(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: The name of the Data Controller as specified in the Addendum or the Agreement.

Address: The address for the Data Controller as specified in the Addendum or the Agreement.

Contact person's name, position and contact details: The contract for the Data Controller as specified in the Addendum or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in DPA

Data importer(s):

Name: Gruntwork, Inc.

Address: The address for the Data Processor is specified in the Agreement.

Contact person's name, position and contact details:The contact details for the Data Processor are specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in the Agreement or the DPA.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Customer's employees and contractors.

Categories of personal data transferred
Customer and Customer's authorized users, which includes Customer's employees and contractors who are granted per-user access rights to Gruntwork's Services, and shall include accounts with such access rights used primarily for performing automated tasks (commonly called "machine users").

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).
Gruntwork will process Customer Information as outlined in Section 2.2 (Customer Instructions), 2.7 (Return or Deletion of Customer Information), and 8 (Modification and Termination of this DPA) of this DPA.

Nature of the processing
Customer Information will be processed in accordance with the Agreement (including this DPA).

Purpose(s) of the data transfer and further processing
To provide the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
Until the termination of the Services or as otherwise instructed by the Data Controller.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
The subject matter, nature, and duration of the processing are described in the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

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

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

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.

The technical and organizational measures (including the certifications held by the data importer) as well as the scope and the extent of the assistance required to respond to data subjects' requests, are described in the DPA.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

The technical and organizational measures that the data importer will impose on sub-processors are described in the DPA.