Data Processing Agreement

This Data Processing Agreement ("DPA") is entered into as of the date of the last signature below, (the "Effective Date"), by and between Gruntwork, Inc., a Delaware corporation with its primary place of business at 221 E. Indianola Avenue, Phoenix, AZ 85012 ("Gruntwork"), and the customer using Gruntwork's platform ("Customer") pursuant to the Gruntwork Terms of Service available at https://gruntwork.io/terms, as updated from time to time, or other agreement between Customer and Gruntwork governing Customer's use of the Service ("the Agreement").

This DPA is incorporated into and forms part of the Agreement. The terms used in this DPA have the meaning set forth in this DPA. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement. Except as modified below, the Agreement remains in full force and effect.

HOW TO EXECUTE THIS DPA

1. This DPA consists of two parts: (i) the main body of the DPA and (ii) Annexes A and B.
2. This DPA has been pre-signed on behalf of Gruntwork.
3. To complete this DPA, Customer must:
    a. complete the information in the signature box and sign on Page 9.
    b. Send the signed DPA to Gruntwork by email to legal.dpa@gruntwork.io.
4. Upon mutual execution of the DPA by Gruntwork and Customer, this DPA will become legally binding.

For the avoidance of doubt, executing this DPA shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Appendices.

HOW THIS DPA APPLIES

Gruntwork provides services to Customer under the Agreement. Pursuant to the Agreement, Gruntwork may from time to time process Personal Data (as defined below) for which Customer may be a "Data Controller" as defined by applicable privacy laws, including the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR").

Because such processing may, from time to time, require the maintenance and implementation of appropriate technical and organizational safeguards, and because such processing may, from time to time, involve the transfer of Personal Data from the European Union to the United States, Customer and Gruntwork have agreed to execute this DPA in order to ensure that adequate safeguards are established with respect to the protection of Personal Data.

1. **Definitions**:

1.1 **"Affiliate"** means an entity that directly or indirectly Controls, or is Controlled by or is under common Control with an entity.

1.2 **"Agreement"** means Gruntwork's Terms of Service or other written or electronic agreement, which govern the provision of the Service to Customer as such terms or agreement may be updated from time to time.

1.3 **"Applicable Data Protection Law"** shall mean all laws and regulations applicable to the processing of personal data under the Agreement. For the sake of clarity, Applicable Data Protection Law includes, without limitation 1) data protection laws and regulations of the European Union, the European Economic Area and their member states and Switzerland; 2) data protection laws and regulations of the United Kingdom; 3) the California Consumer Privacy Act ("CCPA"); 4) the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); and (5) the Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018.

1.4 **"Control"** means an ownership, voting, or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" shall be construed accordingly.

1.5 **"controller"** (controller includes "**Business**" as defined by the CCPA)**, "processor" (**processor includes "**Service Provider**" as defined by the CCPA)**, "data subject" (**data subject includes "**Consumer**" as defined by the CCPA)**, "personal data" (**personal data includes **"Personal Information"** as defined by the CCPA**)** and **"processing"** (and **"process"**) shall have the meanings given in Applicable Data Protection Law.

1.6 **"Customer"** shall mean the Customer entities or Affiliates that are party to the Agreement.

1.7 **"Customer Information"** means any personal data that Gruntwork processes on behalf of Customer via the Gruntwork Services, as more particularly described in this DPA.

1.8 **"EU Data Protection Law"** means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council 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 ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii); and (iii) in respect of the United Kingdom ("UK") any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the UK leaving the European Union.

1.9 **"Europe"** means, for the purposes of this DPA, the European Union, the European Economic Area, and/or their member states, Switzerland, and the United Kingdom.

1.10 **"Gruntwork Services"** shall mean the services Gruntwork is providing pursuant to the Agreement.

1.11 **"SCCs"** mean the standard contractual clauses for processors as approved by the European Commission or Swiss Federal Data Protection Authority (as applicable).

1.12 **"Security Incident"** means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Customer Information on systems managed or otherwise controlled by Gruntwork.

1.13 **"Sensitive Data"** means (a) a social security number, passport number, driver's license number or similar identifier (or any portion thereof); (b) a credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, genetic, biometric, or health information; (d) racial, ethnic, political, or religious affiliation, trade union membership, or information about sexual life or sexual orientation; or (e) other information that falls within the definition of "special categories of data" under applicable Data Protection Laws.

1.14 **"Service Data"** means any data relating to the Customer's use, support, and/or operation of the Service.

1.15 **"Sub-processor"** means any processor engaged by Gruntwork or its Affiliates to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA. Sub-processors may include third parties or Affiliates of Gruntwork, but shall exclude Gruntwork's employees or consultants.

2. **<u>Processing of Personal Data</u>:**

2.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the processing of Customer Information, Customer is the data controller and Gruntwork is the data processor as further described in Annex A (Details of Data Processing) of this DPA. Each party shall comply with its obligations under Applicable Data Protection Law, and this DPA, when processing Customer Information.

2.2 **Customer Instructions.** Gruntwork shall process Customer Information only in accordance with Customer's documented lawful instructions as set forth in the Agreement including this DPA; as necessary to comply with applicable law; or as otherwise agreed in writing ("Permitted Purposes").

2.3 **Prohibited Data.** Customer will not provide (or cause to be provided) any Sensitive Data to Gruntwork for processing under the Agreement and Gruntwork will have no liability

whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this DPA, will not apply to Sensitive Data.

2.4 Customer Obligations. Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Applicable Data Protection Law, in respect of its processing of Customer Information and any processing instructions it issues to Gruntwork; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Applicable Data Protection Law for Gruntwork to process Customer Information for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Information and the means by which Customer acquired Customer Information. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Applicable Data Protection Law) applicable to any content created, sent, or managed through the Service.

2.5 Violations of Applicable Data Protection Law. Customer will ensure that Gruntwork's processing of the Customer Information in accordance with Customer's instructions will not cause Gruntwork to violate any applicable law, regulation, or rule, including without limitation Applicable Data Protection Law. Gruntwork will inform Customer if it becomes aware or reasonably believes that Customer's data processing instructions violate Applicable Data Protection Law.

2.6 Confidentiality Obligations of Gruntwork Personnel. Gruntwork will ensure that any person it authorizes to process the Customer Information shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

2.7 Return or Deletion of Customer Information. Upon Customer's request or upon termination of the Agreement, Gruntwork agrees, at Customer's option, to either deliver to Customer or destroy in a manner that prevents Customer Personal Data from being reconstructed, any Customer Personal Data and any copies in Gruntwork's control or possession, except that this requirement shall not apply to the extent Gruntwork is required by applicable law to retain some or all of the Customer Information or to Customer Information it has archived on back-up systems, which Customer Information Gruntwork shall securely isolate, protect from any further processing, and eventually delete in accordance with Gruntwork's deletion policies, except to the extent required by applicable law.

2.8 No Sale of Information. Gruntwork will not sell Customer Information, nor retain, use, or disclose Customer Information for any commercial purpose other than providing the Gruntwork Services. Gruntwork will not disclose Customer Information outside the scope of the Agreement. Gruntwork understands its obligations under Applicable Data Protection Law and will comply with them.

3. <u>Rights of Data Subjects:</u>

3.1 Data Subject Rights. To the extent Customer, in its ordinary use of the Gruntwork Services, does not have the ability to address a data subject request to exercise his/her rights under Applicable Data Protection Law, Gruntwork shall, upon Customer's request, provide commercially reasonable assistance to Customer in responding to such data subject request.

3.2 Responding to Requests. In the event that any request, correspondence, enquiry or complaint from a data subject, regulator, or third party, including, but not limited to law enforcement, is made directly to Gruntwork in connection with Gruntwork's processing of Customer Information, Gruntwork shall promptly inform Customer providing details of the same, to the extent legally permitted. Unless legally obligated to do so, Gruntwork shall not respond to any such request, inquiry, or complaint without Customer's prior consent. In the case of a legal demand for disclosure of Customer Information in the form of a subpoena, search warrant, court order, or other compulsory disclosure request, Gruntwork shall attempt to redirect the requesting party or agency to request disclosure from Customer. Customer agrees that Gruntwork may provide Customer's basic contact information for this purpose. If Gruntwork is legally compelled to respond to such a request, Gruntwork shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy, unless Gruntwork is legally prohibited from doing so. For the avoidance of doubt, nothing in the Agreement, including this DPA shall restrict or prevent Gruntwork from responding to any data subject or data protection authority requests in relation to personal data for which Gruntwork is a controller.

3.3 Data Protection Impact Assessments. If Gruntwork believes or becomes aware that its processing of Customer personal data is likely to result in a high risk to the data protection rights and freedoms of data subjects, Gruntwork shall inform Customer and (taking into account the nature of the processing and the information available to Gruntwork) provide reasonable cooperation to Customer in connection with any data protection impact assessment or consultations with supervisory authorities that may be required under Applicable Data Protection Law. Gruntwork shall comply with the foregoing by: (i) complying with Section 4.5 (Audits); (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing sub-sections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance at Customer's expense.

4. Security:

4.1 Technical and Organizational Measures. Gruntwork has implemented and will maintain appropriate technical and organizational security measures designed to preserve the security and confidentiality of Customer Information in accordance with Gruntwork's security standards described in Annex B ("Security Measures").

4.2 Updates to Security Measures. Customer is responsible for reviewing the information made available by Gruntwork relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Applicable Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Gruntwork

may update or modify the Security measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Gruntwork Services provided to Customer.

4.3 Security Incident Response. Gruntwork shall, to the extent permitted by law, notify Customer without undue delay of any reasonably suspected or actual Security Incident which affects Customer Information. The notice shall summarize in reasonable detail the nature and scope of the Security Incident, to the extent known, and the corrective action already taken or to be taken by Gruntwork. Furthermore, Gruntwork shall provide timely information relating to the Security Incident as it becomes known or as reasonably requested by Customer and shall promptly take reasonable steps to remedy or mitigate the effect of any Security Incident. Gruntwork's notification of or response to a Security Incident shall not be construed as an acknowledgement by Gruntwork of any fault or liability with respect to the Secuirty Incident. The parties will collaborate on whether any notice of breach is required to be given to any person, and if so, the content of that notice. Unless prohibited by an applicable statute or court order, Gruntwork shall also notify Customer of any third-party legal process relating to any Security Incident, including, but not limited to, any legal process initiated by any governmental entity. Customer agrees that an unsuccessful Security Incident will not be subject to this Section 4.3 (Security Incident Response). An unsuccessful Security Incident is one that results in no unauthorized access to Customer Information or to any of Gruntwork's equipment or facilities used to store or process Customer Information.

4.4 Customer Responsibilities. Notwithstanding the above, Customer agrees that except as provided in this DPA, Customer is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Customer Information when in transit to and from the Gruntwork Services, and taking appropriate steps to securely encrypt or backup any Customer Information uploaded to the Gruntwork Services.

4.5 Audits. Subject to reasonable notice, Gruntwork shall provide Customer an opportunity, at Customer's sole cost and expense, to conduct a privacy and security audit of Gruntwork's security program and systems and procedures that are applicable to the services provided by Gruntwork to Customer. Audits will occur at most annually or following notice of a Security Incident and will be completed in no more than thirty (30) calendar days. If the audit reveals any material vulnerability, Gruntwork shall take commercially reasonable steps to correct such vulnerability.

5. Subcontracting:

5.1 Authorized Sub-processors. Customer agrees that Gruntwork may engage third-party sub-processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf. The sub-processors Gruntwork currently engages to carry out processing activities can be found at https://gruntwork.io/subprocessors. At least 10 days prior to engaging or removing any sub-processor, Gruntwork will update this list and provide Customer with a mechanism to obtain notice of that update. Customer may object in

writing to Gruntwork's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss commercially reasonable alternative solutions in good faith. If the parties cannot reach resolution, Gruntwork will, in its sole discretion, either not appoint such Sub-processor, or permit Customer to suspend or terminate the Agreement without liability to either party.

5.2 **Sub-processor obligations.** Gruntwork shall: (i) conduct appropriate due diligence on each Sub-processor it engages to perform services on its behalf; (ii) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Information as those in this DPA, to the extent applicable to the nature of the service provided by such Sub-processor; and (iii) remain responsible for such Sub-processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-processor that cause Gruntwork to breach any of its obligations under this Agreement.

6. International Transfers of Customer Personal Data:

6.1 Data Center Locations. Customer agrees that Gruntwork may transfer and process Customer Information to and in the United States and any other country where Gruntwork or its Affiliates or Sub-processors conduct operations. Gruntwork shall ensure that such transfers comply with the requirements of Applicable Data Protection Law.

6.2 European Data Transfers. To the extent that Gruntwork receives Customer Information protected by EU Data Protection Laws, Gruntwork agrees to abide by and process such data in compliance with the SCCs, which are incorporated in fully by reference and form an integral part of this DPA. For the purposes of the SCCs: (i) Gruntwork is the "data importer" and Customer is the "data exporter" under the SCCs (notwithstanding that Customer may be an entity located outside the EU); and (ii) Annexes A and B of this DPA shall replace Appendixes 1 and 2 of the SCCs, respectively. For the avoidance of doubt, the SCCs will apply to personal data processed by Gruntwork in the context of providing the Gruntwork Services to Customer that are transferred from Europe to outside Europe, either directly or via onward transfer, to any country or recipient not recognized by the European Commission as providing an adequate level of protection under EU Data Protection Law.

7. Limitation of Liability:

7.1 Liability Cap. Each party and all of its affiliates' liability taken together arising out of or related this this DPA, including the SCCs, shall be subject to the exclusions and limitations of liability set forth in the Agreement.

7.2. Liability to Data Subjects. Each party agrees that it will be liable to data subjects for the entire damage resulting from a violation of Applicable Data Protection Laws. If one party paid full compensation for the damage suffered, it is entitled to claim back from the other party that part of the compensation corresponding to the other party's part of the responsibility for the damage. For that purpose, both parties agree that Customer will be

liable to data subjects for the entire damage resulting from a violation of EU Data Protection Law with regard to processing of personal data for which it is a controller, and that Gruntwork will only be liable to data subjects for the entire damage resulting from a violation of the obligations of EU Data Protection Law directed to processor where it has acted outside of or contrary to Customer's lawful instructions. Gruntwork will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

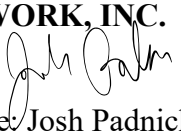
8. **Modification and Termination of this DPA:** This DPA shall remain in effect for so long as Gruntwork processes Customer Information on behalf of Customer or until termination of the Agreement. Failure to comply with any of the material provisions of this DPA is considered a material breach of the Agreement. In the event of termination, Gruntwork will return or destroy data pursuant to Section 2.7 (Return or Deletion of Customer Information). This DPA may only be modified by a written amendment signed by each of the parties.

9. **Entire Agreement; Conflict:** This DPA supersedes and replaces all prior and contemporaneous agreements, oral and written, with regard to the subject matter of this DPA, including any prior data processing addenda entered into between Customer and Gruntwork. If there is any conflict between this DPA and any agreement, including the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) SCCs; then (b) this DPA; then (c) the Agreement.

10. **Service Data:** Notwithstanding anything to the contrary in the Agreement (including this DPA), Gruntwork shall have a right to collect, use, and disclose Service Data for its legitimate business purposes, such as: (i) for accounting, tax, billing, audit, and compliance purposes; (ii) to provide, develop, optimize, and maintain the Service; (iii) to investigate fraud, spam, wrongful or unlawful use of the Service; and/or (iv) as required by applicable law. To the extent such Service Data is considered personal data under Applicable Data Protection Law, Gruntwork shall be responsible for and shall process such data in accordance with the Gruntwork Privacy Policy and Applicable Data Protection Law. For the avoidance of doubt, this DPA shall not apply to Service Data.

11. **Invalidity and Severability.** If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid and unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

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

CUSTOMER	**GRUNTWORK, INC.**
Signature: _____	Signature: 
Customer Legal Name: _____	Print Name: Josh Padnick
Print Name: _____	Title: Director
Title: _____	
Date: _____	Date: September 29, 2020
DPO/Contact for data protection enquiries: _____ _____	DPO/Contact for data protection enquiries: Privacy Team privacy@gruntwork.io

ANNEX A – DETAILS OF PROCESSING

Subject matter:

The subject matter of the data processing under this DPA is the Customer Information.

Duration of the processing:

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.

Purpose:

Gruntwork shall only process Customer Information for the Permitted Purposes, which shall include: (i) processing as necessary to provide the Service in accordance with the Agreement; (ii) processing initiated by Customer in its use of the Service; and (iii) processing to comply with any other reasonable instructions provided by Customer (e.g. via email or support tickets) that are consistent with the terms of the Agreement.

Categories of data subjects:

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").

Types of Customer Information:

Customer may upload, submit, or otherwise provide certain personal data to the Service, the extent of which is typically determined and controlled by Customer in its sole discretion, and may include the following types of personal data:

- Name, email address, profile photo, company name, company address
- Slack and Zendesk details, including URL and admin email address
- Cloud account IDs
- GitHub usernames and repo URLs
- Keybase usernames
- IP addresses

Sensitive Data:

Gruntwork does not want to, nor does it intentionally, collect or process any Sensitive Data in connection with the provision of the Service. However, special categories of data may from time to time be processed through the Services where the Customer or its authorized users choose to include this type of data within the data it transmits using Gruntwork Services. As such, the

Customer is solely responsible for ensuring the legality of any Sensitive Data it or its authorized users choose to process using the Services.

Processing Operations:

Customer Information will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities:

- Storage and other processing necessary to provide, maintain, and improve the service provided to Customer pursuant to the Agreement; and/or

- Disclosures in accordance with the Agreement, Customer's instructions, and/or as compelled by applicable law.

ANNEX B – SECURITY MEASURES

Gruntwork currently observes the following security measures:

1. Organizational Controls

We create a culture of sensitivity around data and security by doing the following:

1. We collect only the minimum data necessary to deliver our services.
2. We ask every employee to make a commitment to protect the secrecy of all internal and customer data.
3. As part of employee onboarding, we ask every employee to read our security policies.
4. As part of employee onboarding, we educate employees about relevant regulations.
5. All critical customer data is stored on systems that have built-in replication, or if necessary, we provide that replication.
6. We maintain a public Google Doc, Gruntwork Security Best Practices, and share it with all employees, customers, and the general public.
7. We conduct a periodic review with our legal team to ensure we are in compliance with all laws and regulations that may apply to us.
8. We have controls in place to maintain the confidentiality of customer information. All Gruntwork employees and contract personnel are bound by Gruntwork's internal policies regarding maintaining confidentiality of customer information and contractually commit to these obligations

2. Authentication Controls

We require that users or employees authenticate to access data by doing the following:

1. Our core business offering includes helping customers secure their physical network infrastructure, and we do this ourselves for any internally hosted data.
2. All access to customer data and internal data requires authentication with a username and password.
3. We require multi-factor authentication for all employees when authenticating to our most important services.
4. We require all employees to store password in a password manager such as 1Password.
5. We require that customers and employees share secrets using pre-approved, secure channels.

3. Authorization Controls

We ensure that only authorized users have access to data by doing the following:

1. We apply the principle of least privilege when granting access to any systems.
2. When storing or processing data using third-party services that allow public access as an option (such as Google Docs), we configure those services to block public access by default.

4. Encryption in Transit

We significantly reduce the likelihood that any data we send across the public Internet is browsed by an unauthorized party by doing the following:

1. We only use third-party services that are available over HTTPS.
2. We never transmit secrets such as passwords or keys over internal chat systems and instead use Keybase to encrypt all such messages.
3. Our limited web services are all available exclusively via HTTPS.

5. Data Integrity & Availability

Because of the limited nature of the data we collect from customers, we have proportionately limited policies in place for ensuring data integrity and availability.

6. Third-Party Considerations

We make sure that data subprocessors that store or process our customers' information themselves practice strong security and data privacy by doing the following:

1. We carefully select our vendors. As part of our vendor review process, we research their record on security.
2. We have a preference for using large vendors for whom a data breach or privacy violation would have grave consequences.
3. We intentionally limit the total number of vendors we use to store or process customer data.
4. We rely on contractual agreements, privacy policies and vendor compliance programs to protect data processed and stored by our third-party vendors.

7. Separation Control

We make sure that data from one customer is not unintentionally combined with that of another customer by doing the following:

1. We minimize the collection of data so that this issue simply does not apply.
2. We maintain oversight of all systems that store customer data by requiring that employees receive express permission from our security team before storing customer data on any new systems.