EU and UK Data Processing Addendum

Confidential

This EU and UK Data Processing Addendum ("DPA") supplements the Workgrounds, Inc. Master Subscription Agreement (the "Agreement") entered into by and between the customer signing this DPA ("Customer") and Workgrounds, Inc. ("Company"). By executing the DPA in accordance with Section 11 herein, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of its Affiliates (defined below), if any. This DPA incorporates the terms of the Agreement, and any terms not defined in this DPA shall have the meaning set forth in the Agreement.

1. Definitions

"Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

"Authorized Sub-Processor" means a third-party who has a need to know or otherwise access Customer's Personal Data to enable Company to perform its obligations under this DPA or the Agreement, and who is either (1) listed in Exhibit B or (2) subsequently authorized under Section 4.2 of this DPA.

"Company Account Data" means personal data that relates to Company's relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account.

"Company Usage Data" means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

"Data Exporter" means Customer.

"Data Importer" means Company.

"Data Protection Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including: (i) the California Consumer Privacy Act ("CCPA"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR") and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR") (together, collectively, the "GDPR"), (iii) the Swiss Federal Act on Data Protection; (iv) the UK Data Protection Act 2018; and (v) the Privacy and Electronic Communications (EC Directive) Regulations 2003; in each case, as updated, amended or replaced from time to time.

"EU SCCs" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 6.2 of this DPA.

"ex-EEA Transfer" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the "EEA"), and such transfer is not governed by an adequacy decision made by the European Commission.

"ex-UK Transfer" means the transfer of Personal Data covered by Chapter V of the UK GDPR, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (the "UK"), and such transfer is not governed by an adequacy decision made by the Secretary of State.

"Services" shall have the meaning set forth in the Agreement.

"Standard Contractual Clauses" means the EU SCCs and the UK SCCs.

"UK SCCs" means the EU SCCs, as amended by the UK Addendum.

2. Relationship of the Parties; Processing of Data

2.1 The parties acknowledge and agree that with regard to the processing of Personal Data, Customer may act either as a controller or processor and, except as expressly set forth in this DPA or the Agreement, Company is a processor. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the processing of such Personal Data.

2.2 Company shall not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this DPA or any other documented instructions provided by Customer, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which the Company is subject, or (iii) in violation of Data Protection Laws. Customer hereby instructs Company to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services.

2.3 The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA.

2.4 Following completion of the Services, at Customer's choice, Company shall return or delete Customer's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law.

2.5 CCPA. Except with respect to Company Account Data and Company Usage Data, the parties acknowledge and agree that Company is a service provider for the purposes of the CCPA (to the extent it applies) and is receiving personal information from Customer in order to provide the Services pursuant to the Agreement, which constitutes a business purpose. Company shall not sell any such personal information. Company certifies that it understands the restrictions of this Section 2.5.

3. Confidentiality

Company shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Company's confidentiality obligations in the Agreement. Customer agrees that Company may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Customer.

4. Authorized Sub-Processors

4.1 Customer acknowledges and agrees that Company may (1) engage its Affiliates as well as the Authorized Sub-Processors listed in Exhibit B to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services. By way of this DPA, Customer provides general written authorization to Company to engage sub-processors as necessary to perform the Services.

4.2 A list of Company's current Authorized Sub-Processors is set forth in Exhibit B of this DPA. At least ten (10) days before enabling any new third party to access or participate in the processing of Personal Data, Company will notify Customer via email. Customer may object to such an engagement by informing Company in writing within ten (10) days of receipt of the notice, provided such objection is based on reasonable grounds relating to data protection.

4.3 If Customer reasonably objects to an engagement in accordance with Section 4.2, and Company cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Company.

4.4 If Customer does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Company, that third party will be deemed an Authorized Sub-Processor for the purposes of this DPA.

4.5 Company will enter into a written agreement with the Authorized Sub-Processor imposing data protection obligations comparable to those imposed on Company under this DPA. In case an Authorized Sub-Processor fails to fulfill its obligations, Company will remain liable to Customer for the performance of the Authorized Sub-Processor's obligations.

5. Security of Personal Data

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, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. Exhibit C sets forth additional information about Company's technical and organizational security measures.

6. Transfers of Personal Data

6.1 The parties agree that Company may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary processing operations take place in the United States (Google Cloud Platform, us-central1 region), and that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer.

6.2 Ex-EEA Transfers. The parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into and incorporated into this DPA by this reference and completed as follows:

> Module One (Controller to Controller) applies when Company is processing Personal Data as a controller pursuant to Section 9 of this DPA.
>
> Module Two (Controller to Processor) applies when Customer is a controller and Company is processing Personal Data for Customer as a processor pursuant to Section 2 of this DPA.
>
> Module Three (Processor to Sub-Processor) applies when Customer is a processor and Company is processing Personal Data on behalf of Customer as a sub-processor.

6.3 For each module, where applicable:

(a) The optional docking clause in Clause 7 does not apply.

(b) In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 4.2 of this DPA.

(c) In Clause 11, the optional language does not apply.

(d) All square brackets in Clause 13 are hereby removed.

(e) In Clause 17 (Option 1), the EU SCCs will be governed by Ireland law.

(f) In Clause 18(b), disputes will be resolved before the courts of Ireland.

(g) Exhibit B to this DPA contains the information required in Annex I and Annex III of the EU SCCs.

(h) Exhibit C to this DPA contains the information required in Annex II of the EU SCCs.

(i) By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

6.4 Ex-UK Transfers. The parties agree that ex-UK Transfers are made pursuant to the UK SCCs, which are deemed entered into and incorporated into this DPA by reference, and amended and completed in accordance with the UK Addendum, which is incorporated herein as Exhibit D of this DPA.

6.5 Transfers from Switzerland. The parties agree that transfers from Switzerland are made pursuant to the EU SCCs with appropriate modifications for Swiss data protection law, including references to the Federal Data Protection and Information Commissioner (FDPIC) as the competent authority.

6.6 Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer: (a) As of the date of this DPA, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies for access to Customer's Personal Data; (b) If the Data Importer receives any such requests, Company shall attempt to redirect the agency to request data directly from Customer and shall give Customer reasonable notice unless legally prohibited; (c) Company shall not voluntarily disclose Personal Data to any law enforcement or government agency.

7. Rights of Data Subjects

7.1 Company shall, to the extent permitted by law, notify Customer upon receipt of a Data Subject Request. If Company receives a Data Subject Request in relation to Customer's data, Company will advise the Data Subject to submit their request to Customer. Customer is solely responsible for responding to such requests.

7.2 Company shall, at the request of the Customer, apply appropriate technical and organizational measures to assist Customer in complying with Data Subject Requests, provided that Customer is itself unable to respond without Company's assistance.

8. Actions and Access Requests; Audits

8.1 Company shall provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under the GDPR to conduct a data protection impact assessment.

8.2 Company shall provide Customer with reasonable cooperation and assistance with respect to Customer's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR.

8.3 Company shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA, and retain such records for a period of three (3) years after the termination of the Agreement.

8.4 Upon Customer's written request at reasonable intervals, Company shall either (i) make available certifications or reports demonstrating compliance, or (ii) allow Customer's independent third party representative to conduct an audit, provided that (a) reasonable prior notice is given; (b) such audit occurs no more than once per calendar year; and (c) such audit is restricted to data relevant to Customer.

8.5 Company shall immediately notify Customer if an instruction, in Company's opinion, infringes Data Protection Laws.

8.6 In the event of a Personal Data Breach, Company shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Company deems necessary and reasonable to remediate such violation.

8.7 In the event of a Personal Data Breach, Company shall provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its notification obligations under the GDPR.

8.8 The obligations described in Sections 8.6 and 8.7 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer.

9. Company's Role as a Controller

The parties acknowledge and agree that with respect to Company Account Data and Company Usage Data, Company is an independent controller, not a joint controller with Customer. Company will process such data as a controller to manage the relationship with Customer, carry out core business operations, monitor and prevent fraud, comply with legal obligations, and provide, optimize, and maintain the Services. Any processing by the Company as a controller shall be in accordance with the Company's privacy policy at https://www.workgrounds.com/privacy.

10. Conflict

In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses; (2) the terms of this DPA; (3) the Agreement; and (4) the Company's privacy policy.

11. Execution of this DPA

Company has pre-signed this DPA. To complete this DPA, Customer must: (i) complete the information requested in the signature block below and sign there, (ii) complete the information requested of the "data exporter" on Exhibit B, and (iii) send the completed and signed Addendum to Company by email to hello@workgrounds.com. Upon receipt of the validly completed Addendum by Company at this email address, this DPA will become legally binding.

Customer	**Workgrounds, Inc.**
Signature: Customer Legal Name:	Signature: Print Name: Nikhil Sethi
Print Name:	Title: CEO
Title:	Date:
Date:	

Exhibit A — Details of Processing

Nature and Purpose of Processing: Company will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's instructions as set forth in this DPA. The nature of processing includes:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Protecting data, including restricting, encrypting, and security testing
- Holding data, including storage, organization, and structuring
- Erasing data, including destruction and deletion
- Sharing data, including disclosure to subprocessors as permitted in this DPA

Duration of Processing: Company will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Company's legitimate business needs; or (iii) by applicable law or regulation.

Categories of Data Subjects: Customer's employees, consultants, contractors, and/or agents who use the Services to book workspaces and travel for corporate events and offsites.

Categories of Personal Data: Name, email address, phone number, job title, company affiliation, payment card information (processed by Stripe), booking and reservation details, travel preferences, IP address, and device identifiers.

Sensitive Data or Special Categories of Data: Customers are prohibited from providing sensitive personal data or special categories of data to Company.

Exhibit B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

1. The Parties

Data exporter(s):

Name: [To be completed by Customer]

Address: [To be completed by Customer]

Contact person: [To be completed by Customer]

Activities: As described in Section 2 of the DPA.

Role: Controller

Data importer(s):

Name: Workgrounds, Inc.

Address: 169 Madison Ave #2384, New York, NY 10016

Contact: hello@workgrounds.com

Activities: As described in Section 2 of the DPA.

Role: As described in Section 2 of the DPA.

2. Description of the Transfer

Data Subjects	As described in Exhibit A
Categories of Personal Data	As described in Exhibit A
Special Category Data	As described in Exhibit A
Nature of Processing	As described in Exhibit A
Purposes of Processing	As described in Exhibit A
Duration and Retention	As described in Exhibit A
Frequency of Transfer	As necessary to provide the Services
Recipients	Authorized Sub-Processors as listed in Section 3 of this Exhibit B

3. Authorized Sub-Processors

Sub-Processor	Purpose	Location
Google Cloud Platform	Cloud infrastructure, hosting, database, and storage	United States
Auth0 (Okta)	User authentication and access management	United States
Stripe	Payment processing for bookings	United States

Intercom	Customer support and in-app messaging	United States
PostHog	Product analytics and usage monitoring	United States
Mailjet	Transactional email delivery	European Union
Duffel	Flight search and booking for event attendees	United Kingdom
Honeycomb	Application performance monitoring and observability	United States

4. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner’s Office.

Exhibit C — Technical and Organisational Security Measures

The following includes the information required by Annex II of the EU SCCs and Annex II of the UK Addendum.

Security Measure	Details
Encryption of personal data	Databases in Google Cloud SQL are encrypted at rest (AES-256). All traffic encrypted in transit (TLS 1.2+). Google Cloud KMS manages all encryption keys.
Confidentiality, integrity, availability, resilience	Customer agreements contain strict confidentiality obligations. Sub-Processors are required to sign comparable confidentiality provisions. Company has maintained SOC 2 Type II certification since 2024, renewed annually (audit cycle begins each February), with continuous compliance monitoring through Vanta.
Ability to restore availability and access	Automated backups of production datastores (Google Cloud SQL) with point-in-time recovery. Infrastructure deployed on Google Kubernetes Engine (GKE) with declarative configurations enabling rapid redeployment.
Regular testing of security measures	Continuous compliance monitoring through Vanta. Automated testing in CI/CD pipeline (Concourse CI) for all production deployments. Regular reviews of security controls and access permissions.
User identification and authorization	Auth0 for user authentication with multi-factor authentication support. Production infrastructure access restricted via Google Cloud IAM with two-factor authentication required.
Protection of data during transmission	All traffic encrypted in transit using TLS 1.2+. All external-facing endpoints served through HTTPS.
Protection of data during storage	Google Cloud Platform default encryption (AES-256) for all persistent storage volumes, Cloud SQL databases, and GCS buckets.
Physical security	All processing occurs in Google Cloud Platform data centers (us-central1, United States). See: https://cloud.google.com/security/infrastructure
Events logging	Application observability through Honeycomb (OpenTelemetry) and GCP Cloud Monitoring. Security-relevant events monitored and investigated by engineering team.
System configuration	Change management process with Concourse CI/CD pipelines. Required code review, automated testing, and staged deployment (staging then production). Infrastructure managed as code using Terraform.

IT security governance	Information security governance program with administrative, organizational, technical, and physical safeguards. Security policies documented and reviewed annually.
Certification/assurance	SOC 2 Type II certified since 2024, renewed annually (audit cycle begins each February). Continuous compliance monitoring through Vanta.
Data minimisation	Company collects only Personal Data necessary to provide the Services. Customers determine what data they provide and have self-service functionality to manage their information.
Data quality	Automated testing in CI/CD pipeline, database schema validation rules, and strongly-typed API to enforce data contracts.
Limited data retention	Customer data deleted upon written request within reasonable timeframe. All Customer Personal Data deleted following service termination.
Accountability	Data protection and information security policies, Personal Data Breach recording and reporting, Record of Processing Activities (ROPA), and formally assigned roles for security and privacy functions.
Data portability and erasure	Personal Data submitted by Customer may be deleted by the Customer or at the Customer's request. Company responds to all data portability requests.
Sub-processor measures	Company enters into Data Processing Agreements with Authorized Sub-Processors with comparable data protection obligations.

Exhibit D — UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter: Customer	Importer: Company
Key Contact	See Exhibit B	See Exhibit B

Table 2: Selected SCCs

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Section 6.2 and 6.3 of the DPA.

Table 3: Appendix Information

Annex 1A: List of Parties	As per Table 1 above
Annex 1B: Description of Transfer	See Exhibit B of this DPA
Annex II: Technical and organisational measures	See Exhibit C of this DPA
Annex III: List of Sub-processors	See Exhibit B of this DPA

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Which Parties may end this UK Addendum	☑ Importer ☑ Exporter ☐ Neither Party

Part 2: Mandatory Clauses

Each party agrees to be bound by the terms and conditions set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs.

Where this UK Addendum uses terms defined in the Approved EU SCCs, those terms shall have the same meaning. This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that together they operate for data transfers made by the data exporter to the data importer where UK Data Protection Laws apply, and they provide Appropriate Safeguards for those transfers.

The following amendments to the EU SCCs apply for the purpose of this UK Addendum:

(a) References to the “Clauses” means this UK Addendum, incorporating the EU SCCs.

(b) References to “Regulation (EU) 2016/679” are replaced by “UK Data Protection Laws.”

(c) References to the “European Union”, “Union”, “EU”, “Member State” are replaced with the “UK.”

(d) The “competent supervisory authority” is replaced with the “Information Commissioner.”

(e) Clause 17 is replaced with: “These Clauses are governed by the laws of England and Wales.”

(f) Clause 18 is replaced with: “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales.”

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

Amendments to the UK Addendum:

From time to time, the ICO may issue a revised Approved UK Addendum. This UK Addendum is automatically amended as set out in any revised Approved UK Addendum from the start date specified. If a party will as a direct result have a substantial, disproportionate and demonstrable increase in costs or risk, and has first taken reasonable steps to reduce those costs or risks, that party may end this UK Addendum at the end of a reasonable notice period.

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