sitestack

Exhibit B – Data Processing Addendum

This Data Processing Addendum ("DPA") is incorporated into and forms part of the Master Subscription Agreement ("Agreement") and applies to the extent SiteStack Processes Customer Personal Data on Customer's behalf in connection with the Services. Capitalized terms not defined in this DPA have the meanings set forth in the Agreement.

1. DEFINITIONS

1.1 Applicable Data Protection Laws. "Applicable Data Protection Laws" means all privacy, data protection, and data security laws and regulations applicable to the Processing of Customer Personal Data, including, where applicable: (a) the EU General Data Protection Regulation and UK GDPR (collectively, "GDPR"); (b) the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA"); (c) other U.S. state privacy laws; and (d) any successor or substantially similar legislation.

1.2 Customer Personal Data. "Customer Personal Data" means any Personal Data included within Customer Data that SiteStack Processes on behalf of Customer under the Agreement.

1.3 Personal Data. "Personal Data" means any information relating to an identified or identifiable natural person.

1.4 Processing. "Processing" or "Process" means any operation or set of operations performed on Personal Data, including but not limited to collection, storage, use, disclosure, transfer, or deletion.

1.5 Subprocessor. "Subprocessor" means any third party engaged by SiteStack to Process Customer Personal Data in connection with the Services.

1.6 Security Incident. "Security Incident" means a confirmed incident resulting in unauthorized access to or disclosure of Customer Personal Data caused by a failure of SiteStack's security measures, excluding unsuccessful attempts that do not compromise Customer Personal Data.

1.7 Standard Contractual Clauses. "Standard Contractual Clauses" or "SCCs" means the European Commission standard contractual clauses (Controller-to-Processor, 2021/914/EU), incorporated by reference into this DPA when required by Applicable Data Protection Laws to legitimize international transfers of Customer Personal Data.

2. ROLES OF THE PARTIES

2.1 Customer as Controller. Customer is the "controller" (or analogous role) of Customer Personal Data, as that term is defined under Applicable Data Protection Laws. Customer determines the purposes and means of Processing of Customer Personal Data.

2.2 SiteStack as Processor. SiteStack Processes Customer Personal Data solely on behalf of Customer as the "processor" (or analogous role) under Applicable Data Protection Laws. For purposes of the CCPA/CPRA, to the extent applicable, SiteStack acts as a "service provider" and/or "contractor" (as such terms are defined under the CCPA/CPRA) with respect to Customer Personal Data.

2.3 Instructions. SiteStack shall Process Customer Personal Data only on Customer's documented instructions. Customer's documented instructions include: (a) the Agreement and this DPA; (b) Customer's use and configuration of the Platform; and (c) other written instructions submitted by Customer through the Platform or via support requests.

3. LIMITATIONS ON PROCESSING

3.1 Purpose Limitation. SiteStack shall Process Customer Personal Data solely to provide the Services and to perform SiteStack's obligations under the Agreement, including to: (a) provide, operate, maintain, and support the Platform and Services; (b) perform API exchanges with Integrated Suppliers as described in Section 11.4 of the Agreement; (c) fulfill operational workflows requested or initiated by Customer through use of the Platform; (d) detect, prevent, investigate, and remediate Security Incidents or technical issues; and (e) comply with SiteStack's legal obligations.

3.2 No Selling or Sharing. To the extent the CCPA/CPRA applies, SiteStack does not sell Customer Personal Data and does not share Customer Personal Data for cross-context behavioral advertising, as those terms are defined under the CCPA/CPRA.

3.3 No Use Outside the Relationship. SiteStack shall not retain, use, or disclose Customer Personal Data for any purpose other than the purposes specified in the Agreement and this DPA, including not for SiteStack's own marketing, targeted advertising, or unrelated commercial purposes. SiteStack shall not attempt to re-identify de-identified data (if any) except as permitted by Applicable Data Protection Laws.

4. CUSTOMER RESPONSIBILITIES

Customer represents, warrants, and covenants that: (a) Customer has provided all notices and obtained all consents, authorizations, and rights necessary for SiteStack to Process Customer Personal Data as contemplated by the Agreement and this DPA; (b) Customer's provision of Customer Personal Data to SiteStack and Customer's instructions for Processing comply with Applicable Data Protection Laws; and (c) Customer will not provide Customer Personal Data to SiteStack except as legally permitted, and will not provide regulated sensitive data types that the Platform is not intended to process unless expressly agreed in writing by the Parties.

5. SECURITY MEASURES

5.1 Security Controls. Taking into account the state of the art, implementation costs, the nature, scope, context, and purposes of Processing, and the risks to individuals, SiteStack implements and maintains administrative, technical, and organizational measures designed to protect Customer Personal Data against unauthorized access, disclosure, alteration, or destruction. Such measures include, at a minimum: (a) role-based access controls and least-privilege principles; (b) encryption in transit using TLS 1.2 or higher; (c) encryption at rest for stored Customer Personal Data; (d) tenant isolation controls, including a separate PostgreSQL database per customer tenant and logical access

controls intended to prevent cross-tenant access; (e) firewalling and network protections; and (f) audit logging of key system events relevant to security and access.
SiteStack may update or modify its security measures from time to time, provided that any such updates do not materially reduce the overall level of protection for Customer Personal Data.

5.2 Personnel. SiteStack shall ensure that personnel authorized to Process Customer Personal Data are subject to appropriate confidentiality obligations (by contract or law) and receive training appropriate to their role. SiteStack shall limit personnel access to Customer Personal Data to those with a need to know for purposes of providing the Services.

6. SECURITY INCIDENT NOTIFICATION

6.1 Notice. Upon becoming aware of a confirmed Security Incident, SiteStack shall notify Customer without undue delay and provide information reasonably sufficient to allow Customer to meet any obligations to notify regulators or individuals under Applicable Data Protection Laws.

6.2 Cooperation. SiteStack shall: (a) investigate the Security Incident and take reasonable steps to contain, mitigate, and remediate its effects; (b) provide Customer with information about the nature of the Security Incident, the categories and approximate number of affected data subjects and records (to the extent known), and the measures taken or proposed to address the Security Incident; and (c) reasonably cooperate with Customer's reasonable requests for further information or assistance related to Customer's legal obligations, provided that such cooperation is limited to information within SiteStack's possession or control and does not require SiteStack to disclose confidential information of other customers or compromise SiteStack's security.

6.3 Exclusions. A Security Incident does not include incidents attributable to Customer, Customer's systems or configurations, Customer's Authorized Users, Customer's vendors, or Integrated Suppliers, except to the extent caused by SiteStack's failure to implement the security measures described in this DPA.

7. SUBPROCESSORS

7.1 Authorization. Customer authorizes SiteStack to engage Subprocessors as necessary to provide the Services, including, by way of example, hosting, infrastructure, email delivery, monitoring, and support tooling providers.

7.2 Obligations. SiteStack shall impose written data protection obligations on its Subprocessors that are no less protective than those set forth in this DPA with respect to the Processing of Customer Personal Data. SiteStack shall remain responsible for the performance of its Subprocessors to the extent required by Applicable Data Protection Laws.

7.3 List of Subprocessors. A current list of Subprocessors will be maintained at: site-stack.com/subprocessors.

7.4 Objection Right. Customer may object to a new Subprocessor on reasonable data protection grounds by providing written notice within a commercially reasonable timeframe after SiteStack posts or provides notice of the new Subprocessor. The Parties shall work in good faith to address Customer's objection, including by considering commercially reasonable alternative arrangements. If the Parties cannot resolve the objection and the affected Subprocessor is required to provide the Services, Customer may terminate the affected Services upon written notice, and any such termination shall be limited to the impacted Services.

8. DATA SUBJECT RIGHTS

To the extent required by Applicable Data Protection Laws, and taking into account the nature of the Processing and the information available to SiteStack, SiteStack shall provide reasonable assistance to Customer in responding to verified requests from data subjects to exercise their rights (including access, deletion, correction, opt-out, and data portability requests) with respect to Customer Personal Data. SiteStack shall not respond directly to a data subject request except: (a) as legally required; or (b) as instructed by Customer in writing. Customer is responsible for verifying the identity of the requesting data subject and for determining whether a request is valid and must be fulfilled.

9. DATA TRANSFERS (GDPR)

9.1 International Transfers. Customer acknowledges that Customer Personal Data may be transferred to, stored in, or accessed from the United States or other countries in which SiteStack or its Subprocessors operate.

9.2 SCCs. Where required under Applicable Data Protection Laws for transfers of Customer Personal Data, the SCCs are incorporated by reference and deemed executed by the Parties, with the following selections and details (to the extent not otherwise specified by the SCCs): (a) Module Two (Controller-to-Processor) applies; (b) Customer is the "data exporter" and SiteStack is the "data importer"; and (c) the Annexes to the SCCs shall be deemed completed using the Processing details set forth in Section 9.4 and the security measures described in Section 5 of this DPA and/or Platform Documentation, as applicable.

9.3 Additional Safeguards. SiteStack implements supplementary measures appropriate to the risk and transfer context, which may include encryption, access controls, audit logging, and data minimization.

9.4 Annex Information.
Nature and Purpose of Processing: Provision of SaaS-based construction procurement, vendor management, workflow automation, analytics, and related Services; platform operation, support, security monitoring, troubleshooting, and Service improvement as permitted by the Agreement and this DPA.
Categories of Data Subjects: Customer employees, contractors, Authorized Users, supplier representatives, and jobsite personnel.
Categories of Personal Data: Contact information, professional identifiers, jobsite location data, transactional procurement records, communications, and usage metadata.

Duration of Processing: For the term of the Agreement and thereafter only as necessary for deletion and backup retention consistent with Section 10.

10. DELETION OR RETURN OF DATA

Upon termination or expiration of the Agreement, SiteStack shall delete Customer Personal Data from production systems within sixty (60) days, unless longer retention is required by applicable law. Customer acknowledges that residual copies of Customer Personal Data may remain in backup systems maintained in the ordinary course of business and will be deleted in accordance with SiteStack's standard backup retention and deletion practices. Upon Customer's written request made on or before termination (or within a commercially reasonable period thereafter), SiteStack will make Customer Personal Data available for export during a thirty (30) day retrieval window in a format consistent with SiteStack's operational practices. For clarity, Aggregated Data (as defined in the Agreement) is not Customer Personal Data and may be retained.

11. AUDITS

Customer may conduct audits no more than once per year, during normal business hours, with thirty (30) days' prior written notice. Customer's audit rights shall be satisfied by SiteStack's provision of relevant security documentation (which may include a SOC 2 report or equivalent summary, if available) and responses to reasonable written questionnaires. On-site audits are permitted only if required by Applicable Data Protection Laws and subject to a mutually agreed scope, timing, confidentiality restrictions, and access limitations designed to prevent disruption of SiteStack operations and protect other customers' data.

11.1 Limitations. Any audit (including any on-site audit) must not: (a) unreasonably disrupt SiteStack operations; (b) permit access to another customer's data or systems; or (c) require disclosure of SiteStack trade secrets or internal source code.

12. MULTI-TENANT ARCHITECTURE

Customer acknowledges and agrees that: (a) the Platform operates on a multi-tenant architecture; (b) Customer Personal Data is stored in a dedicated PostgreSQL database per tenant, and logical access controls are implemented to prevent cross-tenant access; (c) Aggregated Data may incorporate de-identified elements of Customer Data; (d) algorithms and models may utilize Aggregated Data across tenants; and (e) such use of Aggregated Data does not constitute disclosure of Customer Personal Data.

13. API INTEGRATIONS & SUPPLIER DATA EXCHANGE

To the extent SiteStack enables API connectivity with Integrated Suppliers (per MSA §11.4), Customer authorizes SiteStack to exchange operational data reasonably necessary to facilitate procurement, fulfillment, delivery, pickup, billing, service, and related workflows. Customer acknowledges that supplier-generated portal data (e.g., telematics, service updates, unit assignment, and fulfillment status) may be retrieved and displayed to Customer through the Platform. Customer further

acknowledges that SiteStack does not control the independent data practices of third-party suppliers and Integrated Suppliers as such third parties may act as independent controllers/businesses with respect to data they process outside the Platform. For clarity, this exchange is not considered a disclosure of Customer Personal Data to the Marketplace Business, except to the extent operational Order Information is transmitted as expressly permitted by the Agreement.

14. CCPA / CPRA SERVICE PROVIDER OBLIGATIONS

To the extent the CCPA/CPRA applies, SiteStack shall: (a) act solely as a Service Provider and/or Contractor with respect to Customer Personal Data; (b) not sell or share Customer Personal Data; (c) not retain, use, or disclose Customer Personal Data outside the direct business relationship with Customer except as permitted by the Agreement and this DPA; (d) comply with the applicable Service Provider/Contractor requirements under Cal. Civ. Code § 1798.140 and related provisions; and (e) provide reasonable assistance to Customer in responding to verifiable consumer requests as described in Section 8.

15. LIABILITY

Any liability arising out of or related to this DPA is subject to the limitations of liability and exclusions set forth in the Agreement, including any cap, exclusions, and waiver of certain damages, except to the extent such limitations are prohibited by Applicable Data Protection Laws.

16. TERM

This DPA remains in effect for the duration of the Agreement and for so long as SiteStack Processes Customer Personal Data on behalf of Customer, including any period required for deletion and backup retention consistent with Section 10.