Last Updated: 02/21/2023

DATA PROCESSING AGREEMENT

THIS DATA PROCESSING AGREEMENT (this "**DPA**") is incorporated into the Master Services Agreement (the "**Agreement**") between you ("**Service Provider**") and Greystar Management Services, LP, ("**Client**") on the Effective Date of the Agreement.

WHEREAS, the Agreement contemplates that Service Provider will process Personal Information (as defined herein), and therefore, this DPA supplements the Agreement with respect to the collection, use, access to, processing, storage, transmission, disclosure, and destruction of Personal Information by Service Provider under the Agreement.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

1. Relationship to the Agreement

(a) All terms and conditions of the Agreement not otherwise amended by this DPA remain unchanged and in full force and effect and shall govern this DPA. In the event of a conflict between the Agreement and this DPA, the terms and conditions of this DPA shall govern.

(b) The obligations of Service Provider under this DPA shall continue for so long as Service Provider continues to have access to, is in possession of, or acquires Personal Information (the "**Term**"), even if the Agreement between Service Provider and Client is terminated.

2. Definitions

In this DPA, the terms defined in this Section shall have the meanings set out below and other grammatical forms of the same terms shall be construed accordingly. Terms used in this DPA that are not otherwise defined herein or in the Agreement shall have the meaning provided to such terms and similar or analogous terms under Data Privacy Laws, and, for example, Personal Information shall have an analogous meaning to "personal data" where appropriate.

(a) "**Applicable Laws**" means all applicable laws (including those arising under common law), statutes, binding codes, rules, regulations, reporting or licensing requirements, ordinances and other pronouncement having the effect of law in any applicable jurisdiction, including at any national, federal, local, state, county, city or other political subdivision, including those promulgated by any governmental or regulatory authority in effect as of or after the Effective Date and as they may be amended, changed or modified from time to time.

(b) "**Business Purpose**" has its meaning set forth in §1798.140 of the CCPA.

(c) **"Contracted Business Purposes**" means the services provided by Service Provider under the Agreement in which Service Provider receives or accesses Personal Information.

(d) "**Data Privacy Laws**" means all Appliable Laws that govern or regulate the protection, privacy or confidentiality of Personal Information including, to the extent applicable: (i) California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code §§ 1798.100 to 1798.199.95), the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 7000 to 7102), and any related regulations or guidance provided by the California Attorney General ("**CCPA**"); (ii) Colorado Privacy Act ("**CPA**"); (iii) Connecticut's Data Privacy Act "Act Concerning Personal Data Privacy and Online Monitoring (iv) Utah Consumer Privacy Act; and (v) Virginia Consumer Data Protection Act ("**VCDPA**").

(e) "**Personal Information**" means information that identifies, relates to, is or could reasonably be linked, directly or indirectly, with a person. Personal information does not include anonymized, aggregated and deidentified data which is data that in no way identifies or is connected to any person, is impossible to identify individuals within the data sets, and is irreversible.

3. Service Provider Obligations

(a) Service Provider is hereby instructed by Client to process the Personal Information for the Contracted Business Purpose.

(b) Service Provider will impose confidentiality obligations no less restrictive than those Service Provider is subject to on all personnel authorized to process the Personal Information.

(c) Service Provider will only use, retain, or disclose Personal Information for the Contracted Business Purposes for which it collects on behalf of Client or that Client otherwise provides.

(d) Service Provider will not collect, use, retain, disclose, sell, or share Personal Information for Service Provider's own commercial purposes or otherwise in violation of applicable Data Privacy Laws. If Service Provider is legally required to disclose Personal Information for a purpose unrelated to the Contracted Business Purpose, Service Provider must first inform Client of the legal requirement and give Client an opportunity to object or challenge the requirement, unless Applicable Law prohibits such notice.

(e) Service Provider will not sell or share, and shall prohibit by contract any subcontracted party to not sell or share, any Personal Information.

(f) Service Provider will limit Personal Information collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Contracted Business Purposes or another compatible operational purpose.

(g) Service Provider will reasonably assist Client with responding to and fulfilling a Consumer request or instruction requiring Client to provide, amend, transfer, or delete the Personal Information, or to stop, mitigate, or remedy any unauthorized processing.

(h) Service Provider will not combine Personal Information that it receives from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another person, or collects from its own interaction with an individual, provided that Service Provider may combine Personal information to perform any Business Purpose and as set forth in Section 3 (i).

(i) Service Provider may aggregate, deidentify, or anonymize Personal Information and only use such aggregated, deidentified, or anonymized data for its own internal purposes and for the Contracted Business Purposes. Service Provider will not attempt to or actually re-identify any previously aggregated, deidentified, or anonymized data and will contractually prohibit downstream data recipients from attempting to or actually re-identifying such data.

(j) Service Provider will ensure that the Personal Information is transferred in a secure manner.

(k) Service Provider will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks of processing the Personal Information, taking into account in particular the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Information being processed.

4. Assistance with Client’s Data Privacy Law Obligations

(a) Service Provider will reasonably cooperate and assist Client with meeting Client's Data Privacy Law compliance obligations and responding to Data Privacy Law-related inquiries, including responding to verifiable consumer requests, taking into account the nature of Service Provider's processing and the information available to Service Provider.

(b) Service Provider must promptly notify Client immediately if it receives any complaint, notice, communication, or verifiable consumer request that directly or indirectly relates to Client’s compliance with the Data Privacy Laws. Service Provider must notify Client within three (3) working days if it receives a consumer request under the Data Privacy Laws. Service Provider must be able to inform Client as to: (i) the categories and specific pieces of Personal Information collected and/or processed regarding such Consumer; (ii) the categories of sources from which Personal Information was collected; (iii) the categories of third parties with whom Service Provider shares the Personal Information; and (iv) correction or deletion of such consumer's Personal Information. Service Provider shall retain such records for at least twenty-four (24) months after the expiration or termination of the Agreement, whichever longer.

5. Subcontracting

(a) Client authorizes Service Provider to appoint new subprocessors to assist Service Provider with the performance of its obligations under the Agreement on the following conditions. Prior to disclosing Personal Information to any subprocessor, Service Provider shall: (a) provide Client sixty (60) days to object to the proposed subprocessor, which Client shall not unreasonably object; and (b) ensure that such subprocessor has entered into a written agreement with Service Provider requiring that the subprocessor abide by terms no less protective than those provided in this DPA.

(b) If Client has a reasonable basis to object to the use of any subprocessor, Client shall notify Service Provider. In the event Client objects to a subprocessor, Service Provider shall make available a change in the services or use of the affected services to avoid processing of Personal Information by the objected-to subprocessor. Any such change shall be subject to prior agreement by Client, such agreement shall not be unreasonably denied or delayed. As between Client and Service Provider, Service Provider shall remain fully liable for all acts, omissions, and obligations of any subprocessor appointed by it pursuant to this DPA.

(c) If Service Provider is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Client may terminate those services which cannot be provided by Service Provider without the use of the objected-to sub-processor, by providing written notice. Such termination shall be without penalty to Client, and where Client has prepaid for such services, Client shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated services. At all times, Service Provider shall maintain a current list of approved subprocessors.

6. Warranties

(a) Service Provider represents and warrants that it complies and will maintain in compliance with Applicable Law and all applicable requirements of the Data Privacy Laws when collecting, using, retaining, or disclosing Personal Information.

(b) Service Provider warrants that it has no reason to believe any Data Privacy Laws' requirements or restrictions prevent it from providing any of the Contracted Business Purposes or otherwise performing under the Agreement. Service Provider must promptly notify Client of any changes to the Data Privacy Laws' requirements that may adversely affect its performance under the Agreement.

7. Audit

(a) Client may implement requirements and/or take reasonable steps to ensure that Service Provider, and any subprocessors, process the Personal Information in a manner consistent with this DPA and Client's obligations under applicable Data Privacy Laws. If Client implements any requirements or steps that Service Provider and/or any subprocessors must meet, Client shall provide notice at least fifteen (15) days prior to the effective date of such requirements. Service Provider may request up to thirty additional days to implement such requirements, of which Client shall not unreasonably deny.

(b) Service Provider shall retain records and information sufficient to audit and verify its compliance with this DPA and the Data Privacy Laws. Upon reasonable notice, Service Provider shall submit to a review of Service Provider's systems, records, and facilities for the purpose of verifying compliance with this DPA and Client requirements. Service Provider shall provide Client its auditors (including internal audit staff and external auditors), inspectors and regulators with access to its site, system, and records as reasonably necessary to assess compliance with this DPA. Such audit will be conducted at Client's sole expense, unless it reveals a material non-compliance with the requirements of this DPA or Client requirements, in which case the cost shall be borne by Service Provider.

(c) Service Provider shall provide to Client, its auditors (including internal audit staff and external auditors), inspectors and regulators, access at all reasonable times to any location processing Personal Information, to Service Provider employees, and to data and records relating to the services for the purpose of performing audits and inspections of either Service Provider or any of its subprocessor to: (a) verify the security and integrity of Personal Information; (b) examine the systems that process Personal Information or that are used to perform the services and examine any external Service Provider processing and security audits, reports or reviews; and (c) verify whether the services Service Provider security practices comply with the Data Privacy Laws and the requirements of this DPA.

(d) Service Provider shall provide full cooperation to Client and its auditors, and Service Provider shall require its subcontractors to comply with the provisions of this Section. Service Provider's obligations under this Section 7(d) shall extend for a period of four (4) years beyond the term of the Agreement, unless Applicable Law mandates a longer period.

8. Retention and Deletion of Data

(a) Service Provider shall only retain Personal Information for as long as necessary for Service Provider to perform its obligations under the Agreement and this DPA. For the avoidance of doubt, this shall not limit the retention of information pursuant to Section 3 (i).

(b) Upon the expiration or earlier termination of the Agreement or until Service Provider is no longer providing the services to Client with respect to Personal Information, whichever later Service Provider shall, at the direction of Client, return or destroy all Personal Information covered by the services, unless such information is aggregated and anonymized or required to be held by Service Provider under Applicable Law. Service Provider must make all Personal Information available to Client within ten (10) days after the expiration or earlier termination of the Agreement.

9. Security Breach Reporting & Cooperation

(a) Notification of Security Breach. In the event that Service Provider reasonably suspects an unauthorized access, acquisition, disclosure, or use of Personal Information maintained pursuant to the Agreement (each such occurrence, a "**Security Breach**"), Service Provider shall, to the extent permitted by law, promptly and without undue delay notify Client in writing at:

(i) **Client:**
[ADDRESS]
[ADDRESS]
[ATTN:]

Notification shall be provided to Client no later than later than five (5) days after reasonably suspecting such Security Breach. In the event that Service Provider becomes aware a Security Breach has occurred or is ongoing, Service Provider shall, to the extent permitted by law, promptly and without undue delay notify Client no later than twenty-four (24) hours after becoming aware of the Security Breach.

Such notification shall include, to the extent known, following a reasonable inquiry carried out in accordance with Service Provider's internal breach response procedures, all information in its custody or under its control on (i) the extent and nature of the Security Breach, including the categories and volume of affected Personal Information, (ii) the estimated risks and likely consequences of the Security Breach to each party, and (iii) the investigative, corrective, and remedial actions taken, planned, or proposed to prevent, contain, mitigate, and remediate the Security Breach.

(b) Root Cause Analysis. Service Provider shall promptly, and at its own expense, perform an analysis of the Security Breach to diagnose problems at a level of reasonable detail such that all problems can be accurately and completely identified and corrective action can be taken to eliminate repeated failures to the maximum extent reasonably possible ("**Root Cause Analysis**"). Service Provider shall provide regular updates on the progress of, and developments relating to, such Root Cause Analysis and shall provide a written report containing its associated findings and recommendations to Client within no more than fifteen (15) business days of confirming the Security Breach.

(c) Cooperation. The parties shall promptly and continuously cooperate, including any designated representatives and any third parties contracted to advise on investigative, corrective, or remedial actions on Service Provider's efforts to prevent, contain, mitigate, and remediate the Security Breach, which may include responding to reasonable requests for relevant information, data, or records by each other and by law enforcement or other governmental authorities in accordance with the confidentiality requirements herein. Those efforts shall include input from each party's designated representatives and third parties contracted to advise on investigative, corrective, or remedial actions on the notifying party's efforts. Service Provider shall use best efforts to collect and preserve all evidence relating to the Security Breach and to document its investigative, corrective, and remedial actions in detail. At Client's request from time to time, Service Provider shall provide Client with reasonable written assurances that the Security Breach is not likely to recur. If a Security Breach occurs for any reason, Client may elect in its discretion to terminate immediately Service Provider's provision of products and/or services under the Agreement and have not obligation to pay Service Provider any additional amounts.

(d) Third-Party Notifications. At Client's request, Service Provider shall provide written notice, in a manner and format Client approves, to all individuals whose Personal Information was affected by the Security Breach and to any other third parties, such as regulators, law enforcement agencies, and consumer reporting agencies, that Client determines should be notified of the Security Breach, in its sole discretion, except Service Provider shall not be limited in reporting criminal activity or as may otherwise be required by law. Service Provider shall bear all reasonable costs associated with all notifications to affected individuals and other entities required by law, in addition to all reasonable costs of any other Security Breach remediation efforts required by law, including providing credit monitoring or identity theft services to affected individuals and establishing a call center.

10. Data Ownership

Service Provider shall have no ownership rights or interest in Personal Information and acknowledges that Client is the owner of any and all Personal Information.

11. Insurance

(a) Insurance Coverage. Service Provider shall carry, at its sole cost and expense, the following insurance, in a form and with insurers acceptable to Client, under a policy rated A- or better by Best's Key Rating Guide:

(i) Professional Liability Insurance covering the errors and omissions of Service Provider, Service Provider personnel and Service Provider subcontractors in relation to the services performed and Service Provider 's obligations under this DPA. Such policy shall have a per claim and annual aggregate limit of at least $5,000,000.

(ii) Cyber Insurance coverage, including network security, cyber-attack and web content liability; failure to prevent a party from unauthorized access to, unauthorized use of, tampering with or introduction of malicious code into data systems, or failure to properly handle, manage, store, destroy, or otherwise control Personal Information in any format; having a per claim and annual aggregate limit of $10,000,000. This insurance shall also include coverage for, but not be limited to, the cost to mitigate claims, including cost of customer credit monitoring and cost of customer notification; and the cost of regulatory fines or other statutory damages under Data Privacy Laws. The network security, cyber-attack, and web content liability portion of such policy shall name Client, its clients, and each of their Affiliates as additional insureds against Service Provider claims arising from the actions of Service Provider's representatives.

(iii) Employee Dishonesty and Computer Fraud insurance with limits of at least $5,000,000 per loss. Such policy shall include a Third-Party Coverage Endorsement for theft of money, securities or other client-tangible property that Service Provider holds or for which Service Provider is legally liable, resulting from dishonest acts committed by employees of Service Provider or its contractors in the performance of services under the Agreement and the Processing of Personal Information under this DPA. Such Service Provider /client coverage shall also include a loss payable clause in favor of Client and its Affiliates.

(b) Insurance Terms. The insurance described in Section 9 (Insurance) shall (a) be primary and non-contributing in nature to any insurance maintained by Client or its clients and (b) shall waive all the insurers and insureds' individual and/or mutual rights of subrogation against Client, its clients, and each of their Affiliates. Certificates shall be kept current and in compliance throughout the Term of this DPA and Service Provider shall provide Client with 30 days' advance written notice to Client in the event of cancellation or material change adversely affecting the interests of Client. If any coverage is written on a claims-made basis, coverage with respect to work performed under this DPA and the Agreement shall be maintained for a period of at least three years after the expiration or termination of the Agreement, or if no Agreement is in effect between the parties, of this DPA.

12. Miscellaneous

(a) Incorporation. This DPA is effective as of the Effective Date of the Agreement between you and Client and is incorporated into such Agreement by reference. You acknowledge and agree that this DPA is identifiable beyond all reasonable doubt as the document incorporated into the Agreement via the URL link to this DPA in the Agreement.

(b) Governing Law and Jurisdiction. This DPA shall have the same governing law and jurisdiction as the Agreement. In the event the Agreement does not identify or address the governing law or jurisdiction, then, this DPA shall be construed in accordance with and governed by the internal laws of the State of Delaware, without regard to the principles of conflicts of law. Any action based upon, arising out of or related to this DPA may be brought in the federal courts located in the State of Texas, and each of the parties irrevocably submits to the exclusive jurisdiction of such court in any action, waives any objection it may now or hereafter have to personal jurisdiction, venue or to convenience of forum, agrees that all claims in respect of the action shall be heard and determined only in any such court, and agrees not to bring any action arising out of or relating to this DPA in any other court. Each of the parties hereby irrevocably waives any and all right to trial by jury in any action based upon, arising out of or related to this agreement or the transactions.

(c) Notices. Any notices, demands, consents, approvals and other communications necessary or provided for under this DPA shall be in writing and shall be addressed and sent to the addresses specified in the Agreement and in accordance with the notice provisions set forth in the Agreement.

(d) Severability. Each provision of this DPA is intended to be severable. If any term or provision hereof or the application thereof to any party or circumstance shall be determined by a court of competent jurisdiction to be invalid, illegal or unenforceable for any reason whatsoever, such term, provision or application thereof shall be severed from this DPA and shall not affect the validity of the remainder of this DPA or the application of such term or provision to any other party or circumstance.

(e) Waiver. No consent or waiver, express or implied, by either party to or of any breach or default by the other party in the performance of its obligations hereunder, shall be valid unless in writing and signed by the party against whom such waiver is sought to be enforced. No such consent or waiver shall be deemed or construed to be a consent or waiver to or of any other breach or default in the performance by such other party of any other obligations of such party hereunder. The failure of any party to declare the other party in default shall not constitute a waiver by such party of its rights hereunder, regardless of how long such failure continues.

(f) Assignment. The rights and obligations of Service Provider hereunder may not be assigned without the prior written consent of Client. In the event of such consented assignment, the assignee shall assume all obligations of the assigning party, and the assigning party shall be released from all liabilities hereunder arising from and after any such permitted assignment. This DPA shall inure to the benefit of, and constitute a binding obligation upon, the parties hereto and their respective successors and permitted assigns.

(g) Entire Agreement; Amendment. This DPA contains the entire agreement between the parties hereto with respect to the subject matter hereof and supersedes all prior oral or written agreements, understandings, representations, and covenants. This DPA may be amended from time to time by Client by posting an updated version to the URL and noting when the document was last updated. The DPA may not otherwise be amended, supplemented, or modified by Service Provider except by an agreement in writing signed by the parties.

(h) Interpretation. No provision of this DPA shall be construed against or interpreted to the disadvantage of either party by any court or other governmental, judicial or arbitral authority by reason of either party having, or being deemed to have, structured or dictated such provision. The parties hereto acknowledge that the parties have jointly participated in the negotiation and preparation of this DPA.

(i) Headings. The headings in this DPA are for reference only and shall not affect in any way the meaning or interpretation of this DPA.

(j) Survival. The obligations of Service Provider under Section 3 (Service Provider Obligations) Section 6 (Warranties), Section 7 (Audit), Section 9 (Security Breach Reporting & Cooperation), Section 10 (Data Ownership), Section 11 (Insurance), Section 12 (Miscellaneous), and any other provisions of this DPA which by their terms are stated to survive the termination of this DPA shall survive the expiration or termination of this DPA by any party and are not extinguished as a result of the expiration or termination of this DPA, regardless of the circumstances of termination.

(k) Authority. The undersigned parties have each been duly authorized and have all the requisite power to execute this DPA. The parties represent and warrant to each other that all terms and conditions of this DPA are binding upon and enforceable against the parties.