Revinate Data Processing Addendum

This Revinate Data Processing Addendum ("DPA") is incorporated by reference into the agreement between Revinate and Customer (the "Agreement") regarding Revinate's hospitality management services ("Services"). This DPA is entered into as of the later of the dates beneath the parties' signatures below. Capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement.

This DPA is supplemental to the Agreement and sets out the terms that apply when Personal Data (defined below) is processed by Revinate under the Agreement. The purpose of the DPA is to ensure such processing is conducted in accordance with EU Data Protection Legislation.

HOW TO EXECUTE THIS DPA

This DPA has been pre-signed on behalf of the applicable Revinate entities. When Revinate receives the completed and signed DPA, this DPA will become a legally binding addendum to the Agreement. To make this DPA a part of the Agreement, Customer must complete the information in the signature block of this DPA and have an authorized representative sign on page 6. Please return the signed copy to Revinate via email at: support+privacy@revinate.com.

HOW THIS DPA APPLIES

A. If the Customer entity signing this DPA is a party to the Agreement, the Revinate entity that is a party to the Agreement is a party to this DPA.

B. If the Customer entity signing this DPA has executed orders under the Agreement but is not a party to the Agreement, this DPA will be incorporated in such order(s) and the Revinate entity that is a party to such order(s) will be a party to this DPA. For avoidance of doubt, this means that if a property or group has purchased Revinate, where that property or group's larger parent or affiliate signed an Agreement with Revinate, this Addendum may still apply to the property or group.

C. This DPA is not a standalone agreement. Revinate has no obligations as to any entity that does not have an executed Agreement with Revinate, even if that entity signs this DPA.

1 Definitions

For the purposes of this DPA:

1.1 "Affiliate(s)" has the same meaning ascribed to it in the Agreement and, if not defined in the Agreement, the term means any legal entity directly or indirectly controlling, controlled by or under common control with a party, where control means the ownership of a majority share of the stock, equity or voting interests of such entity.

1.2 "CCPA" means the California Consumer Privacy Act, its associated regulations and their successors.

1.3 "Controller," "Processor", "Data Subject," "Personal Data," "Processing" and "Process" (whether or not capitalized) have the meanings ascribed to them by EU Data Protection Legislation and include equivalent terms in the CCPA.

1.4 "Customer" means the non-Revinate party to both the Agreement and this DPA that has access to the Services.

1.5 “Customer Data” means any data, information or material originated by Customer that Customer submits to Revinate, collects through its use of the Services or provides to Revinate in the course of using the Services.

1.6 “EEA” means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland, Liechtenstein, the United Kingdom and Switzerland.

1.7 “EU Data Protection Legislation” means 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, and repealing Directive 95/46/EC (“General Data Protection Regulation” or “GDPR”), as amended, replaced or superseded.

1.8 “Personal Data”: (a) has the meaning provided in EU Data Protection Law in reference to residents of the European Economic Area, and (b) means Personal Information as defined in the CCPA in reference to California residents, and (c) in reference to residents of other jurisdictions incorporates equivalents terms under other laws applicable to the Services.

1.9 “Revinate” means the Revinate entity that is a party to both the Agreement and this DPA, which may be Revinate, Inc., a Delaware corporation, or a Revinate Affiliate as applicable.

1.10 “Security Incident” means accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access or use of Personal Data stored in the Services.

2 Applicability of DPA

2.1 In providing the Services to Customer pursuant to the Agreement, Revinate may process Personal Data on behalf of Customer. Revinate will comply with the provisions in this DPA with respect to its processing of any Personal Data.

2.2 Sections 3, 4 and 8 - 11 govern Revinate’s processing of all Personal Data from anywhere in the world. Section 5 applies only to the extent Customer is established within the EEA and/or to the extent Revinate processes Personal Data of Data Subjects located in the EEA on behalf of Customer or a Customer Affiliate. Section 6 applies only to personal data of California residents.

3 Global Processing Terms.

3.1 General Processing Conditions. Revinate shall process Customer Data provided by Customer for the purposes set forth in the Agreement and only in accordance with the lawful, documented instructions of Customer, except where otherwise required by applicable law. Revinate may have a separate right to process certain Personal Data: (a) if Revinate receives the same guest Personal Data from multiple customers, and (b) if Revinate has a direct relationship with a data subject and is a controller of that Personal Data.

3.2 Compliance. Customer is responsible for ensuring that: (a) its use of the Services complies with all applicable laws relating to privacy and data protection, including EU Data Protection Legislation and the CCPA; and (b) it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to Revinate for processing in accordance with the terms of the Agreement and this DPA.

3.3 Training. Revinate shall ensure that its relevant employees, agents and contractors receive appropriate training regarding their responsibilities and obligations with respect to the processing, protection and confidentiality of Customer Data.

4 Security

4.1 Security. Revinate shall implement appropriate technical and organizational measures designed to prevent Security Incidents.

4.2 Confidentiality of Processing. Revinate shall ensure that any person that it authorizes to process the Personal Data (including its staff, agents and subcontractors) shall be subject to a duty of confidentiality (whether a contractual or a statutory duty) that shall survive the termination of their employment and/or contractual relationship.

4.3 Security Incidents. Upon becoming aware of a Security Incident, Revinate shall notify Customer without undue delay and pursuant to the terms of the Agreement, but within no more than 48 hours, and shall provide such timely information as Customer may reasonably require to enable Customer to fulfill any data breach reporting obligations under EU Data Protection Legislation. Revinate will take steps to immediately identify and remediate the cause of such Security Incident if caused by Revinate.

4.4 Processing in Accordance with California Law. In accordance with the CCPA, and with respect to Personal Data to which CCPA applies: (a) Contractor will not "sell" (as defined in the CCPA) any Personal Data; and (b) Revinate will not collect, share or use any Personal Data except as necessary to perform services for Customer.

5 EEA-Specific Processing Terms

5.1 Processing in Accordance with EU Law. Customer may be the controller of Personal Data or a processor. Revinate will act as a processor or sub-processor, as appropriate. Each party will comply with the obligations that apply to it under EU Data Protection Law. Revinate will promptly inform Customer if it becomes aware that processing requested by Customer infringes EU Data Protection Law.

5.2 Sub-processors. Customer agrees that Revinate may engage Revinate Affiliates and reputable third party subprocessors (collectively, "Sub-processors") to process the Personal Data on Revinate's behalf. The Sub-processors currently engaged by Revinate and authorized by Customer are listed at Revinate's Sub-processor web page (the "Sub-processor List"): https://www.revinate.com/subprocessors. Revinate shall impose on such Sub-processors data protection terms that protect the Personal Data to the same standard provided for by this DPA. Where a Sub-processor fails to fulfil its data protection obligations, Revinate shall remain liable to Customer for the performance of that sub-Processor's obligations.

5.3 Changes to Sub-processors. Revinate will inform Customer of any intended changes concerning the addition or replacement of Sub-processors and within ten days after being notified of the engagement of the Sub-processor, Customer may object to such changes on reasonable grounds relating to the protection of the Personal Data. In such case Revinate shall have the right to cure the objection through one of the following options (to be selected at Revinate's sole discretion): (a) Revinate will cancel its plans to use the Sub-processor with regard to Personal Data or will offer an alternative to provide the Services without such Sub-processor; or (b) Revinate will take the corrective steps requested by Customer in its objection (which remove Customer's objection) and proceed to use the Sub-processor with regard to Personal Data; or (c) Revinate may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the Services that would involve the use of such Sub-processor with regard to Personal Data. Objections to a Sub-processor must be submitted to Revinate by following the directions set forth in the Sub-processor List. If none of the above options are reasonably available and the objection has not been resolved to the mutual satisfaction of the parties within 30 days after Revinate's receipt of Customer's objection, either party may terminate the Agreement. Customer will not receive a refund of any unused prepaid fees on such termination and if fees remain unpaid for a subscription term Customer will immediately pay the remaining balance due for the remained of the subscription term.

5.4 Emergency Replacement. Revinate may replace a Sub-processor if the reason for the change is beyond Revinate's reasonable control. In such instance, Revinate shall notify Customer of the replacement as soon as reasonably practicable, and Customer shall retain the right to object to the replacement Sub-processor pursuant to Section 5.3 above.

5.5 Transfers Outside the EEA. Revinate may not transfer Personal Data to, or process such data in, a location outside of the EEA without Customer's prior written consent (in each case a "Transfer"). Without prejudice to the foregoing, Customer consents to Transfers outside of the EEA where Revinate has implemented a Transfer solution compliant with EU Data Protection Legislation, which for example may include: (a) where such Transfer is subject to an adequacy decision by the European Commission; (b) the unchanged European Commission-approved controller to processor Standard Contractual Clauses (without optional clauses) set out at http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm as of the date of this DPA or any successor thereto adopted in accordance with GDPR ("SCCs"), which are incorporated by reference into this DPA, where Customer will be regarded as the Data Exporter and Revinate will be regarded as the Data Importer; (c) another appropriate safeguard pursuant to Article 46 of the GDPR applies; or (d) a derogation pursuant to Article 49 of the GDPR. Appendices 1 and 2 of this DPA correspond to Appendices 1 and 2 of the SCCs. Provisions of this DPA will supersede the SCCs to the extent of any conflict.

6 California-Specific Processing Terms

6.1 Processing in Accordance with California Law. In accordance with the CCPA, and with respect to Personal Data to which CCPA applies: (a) Contractor will not "sell" (as defined in the CCPA) any Personal Data; and (b) Revinate will not collect, share or use any Personal Data except as necessary to perform services for Customer.

7 Cooperation with Data Subject Right Requests

7.1 Data Subjects' Rights. Revinate shall provide commercially reasonable assistance, including by appropriate technical and organizational measures as reasonably practicable, to enable Customer to respond to any inquiry, communication or request from a Data Subject seeking to exercise his or her rights under EU Data Protection Legislation and the CCPA, including rights of access, correction, restriction, objection, erasure or data portability, as applicable.

7.2 Data Subject Requests. In the event such inquiry, communication or request is made directly to Revinate, Revinate shall promptly inform Customer by providing the full details of the request. For the avoidance of doubt, Customer is responsible for responding to Data Subject requests for access, correction, restriction, objection, erasure or data portability of that Data Subject's Personal Data.

7.3 Data Protection Impact Assessments and Prior Consultation. Revinate shall, to the extent required by EU Data Protection Legislation, provide Customer with reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out under EU Data Protection Legislation.

8 Security Reports and Audits.

Revinate will make available to Customer such information as Customer may reasonably request to demonstrate Revinate's compliance with the obligations under EU Data Protection Legislation. Revinate will further allow for and contribute to audits conducted by Customer or an auditor mandated by Customer so long as it is not a competitor of Revinate. All such information and audit requests and procedures: (a) must be reasonable based on the nature of the Services and the categories of Personal Data processed, (b) must be subject to an appropriate confidentiality agreement; and (c) may be made no more than once per year unless otherwise required by instruction of a competent data protection authority. If the Agreement does not include audit rights, Revinate and Customer will discuss and agree in advance on the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit; and Revinate reserves the right to charge a fee (based on Revinate's reasonable costs) for any such audit. Revinate will provide further details of any applicable fee and the basis of its calculation to Customer in advance of such audit.

9 Deletion or Return of Customer Data

9.1 Deletion or Return of Data. Upon termination or expiration of the Agreement, Revinate shall, upon customer's written request and in accordance with the terms of the Agreement, delete or make available to Customer for retrieval all relevant Personal Data (including copies) in Revinate's possession. Notwithstanding the foregoing, Revinate may retain copies of Personal Data that cannot reasonably be returned, destroyed or deleted, such as email back-up records, back-up server tapes and similar automated record-keeping or other retention systems. The receiving party shall: (a) continue to extend the protections of this section to such Confidential Information and limit further use and disclosure of such Confidential Information to those purposes that make the return or destruction of such Confidential Information infeasible, and (b) comply with the preceding paragraph as soon as permitted under applicable laws or recipient's internal record retention policy.

10 Customer Security Measures.

10.1 Customer Responsibilities. Customer is responsible for security relating to its environment and security relating to configuration of the Services. This includes implementing and managing procedural, technical, and administrative safeguards on the Services, Customer's networks, databases and guest management systems sufficient to: (a) ensure the confidentiality, security, integrity, and privacy of Customer Data in transit, at rest, and in storage; (b) protect against any anticipated threats or hazards to the security and integrity of Customer Data; and (c) protect against any unauthorized processing, loss, use, disclosure or acquisition of or access to Customer Data. Notwithstanding any other provision of this DPA, the Agreement or any other agreement related to the Services, Revinate will have no obligations or liability as to any breach or loss resulting from: (x) Customer's environment, databases, systems or Services, or (y) Customer's security configuration or administration of the Services.

10.2 Appropriate Permissioning. Customer is solely responsible for provisioning users on the Services, including: a) setting the right access for the users b) managing user access privileges c) deauthorizing personnel who no long need access to the services d) regularly auditing access to the Services e) regularly auditing any public access links users create and restricting the permission to create public links, as necessary.

11 Miscellaneous

11.1 Except as amended by this DPA, the Agreement will remain in full force and effect.

11.2 If there is a conflict between the Agreement and this DPA, the terms of this DPA will control.

11.3 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations of liability set forth in the Agreement.

11.4 This DPA will be governed by and construed in accordance with the laws of the jurisdiction governing the Revinate Services Agreement unless otherwise required by EU Data Protection Legislation, in which case this DPA will be governed by the laws of the Netherlands.

[SIGNATURE PAGE FOLLOWS]

ACCEPTED AND AGREED TO:

Customer: ____________________________

Legal Name of Customer

Signed By:

Signature: ______________________

Print Name: ______________________

Title: ______________________

Date: ______________________

Revinate, Inc.

Signed By:

Signature: ______________________

Print Name:

Title: Chief Revenue Officer

Date: ______________________

APPENDIX 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

Revinate processes Personal Data in order to provide its services to hospitality customers as described at www.revinate.com

Duration of Processing

Revinate will process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Categories of Data Subjects

The personal data transferred concern the following categories of data subjects (please specify):

The data importer's services may have access to personal data regarding EEA citizens who: (a) work for the data exporter and set up user accounts on Revinate's services, and (b) are guests at the data exporter's properties.

Type of Personal Data

The Revinate services will have access to the names and email addresses of Customer personnel who log in to the Revinate service.

The personal data transferred concern categories of data related to a guest's hotel stay or other visit, including:

- Name
- Email address
- Physical address
- IP-address and other online identifiers
- Date of birth
- Telephone/mobile number
- Location Data
- Information related to a guest's hotel reservation and stay

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Revinate's services will process the categories of personal data provided by the data importer. If the data importer's property management system captures special categories of data, including without limitation factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity, and the data importer chooses to make those categories available to Revinate, Revinate may process them.

APPENDIX 2 – SECURITY CONTROLS

Description of Revinate's Technical and Organisational Security Measures

1. System Access Controls: data importer shall take reasonable measures to prevent personal data from being used without authorization. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.

2. Data Access Controls: data importer shall take reasonable measures to provide that personal data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the personal data to which they have privilege of access; and, that personal data cannot be read, copied, modified or removed without authorization in the course of processing.