

This Data Processing Addendum (“**Addendum**”) forms part of the agreement between the undersigned customer (“**Customer**”) and Kyriba for the purchase of online services from Kyriba (the “**Agreement**”) to reflect the parties’ agreement with regard to the processing of Customer Personal Data and replaces and supersedes any existing provision regarding Customer Personal Data in the Agreement. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. The parties understand that personal information may be processed by Kyriba on behalf of Customer (“**Customer Personal Data**”). Customer Personal Data includes information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to, directly or indirectly, a particular individual, consumer, data subject, or household, or is defined as “personally identifiable information,” “personal information,” “personal data,” or similar term under Applicable Data Protection Law. “**Applicable Data Protection Law**” means, if and to the extent applicable, (a) the UK Data Protection Act 2018; (b) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 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**”); (c) as of January 1, 2020, the California Consumer Privacy Act of 2018, California Civil Code § 1798.100 *et seq.* (“**California Consumer Privacy Act**” or “**CCPA**”); and (d) any other data protection laws, rules, regulations, self-regulatory guidelines, or implementing legislation applicable to Kyriba’s processing of Customer Personal Data. Words and phrases in this Addendum shall, to the greatest extent possible, have the meanings given to them in Applicable Data Protection Law. The parties acknowledge and agree that Customer is the controller or business that determines the purpose for and the manner in which Customer Personal Data is processed by Kyriba. The parties agree that control of and responsibility for such Customer Personal Data shall at all times remain with Customer, Kyriba is the processor or service provider that processes Customer Personal Data under this Addendum and according to Customer’s instructions.

2. Kyriba will process Customer Personal Data in accordance with Applicable Data Protection Law and solely for the purpose of providing the SaaS Services to Customer. Kyriba will not otherwise (i) process Customer Personal Data for purposes other than those set forth in this Addendum or as instructed by Customer’s documented written instruction; (ii) disclose Customer Personal Data to third parties other than Kyriba’s affiliates or subsidiaries, for the aforementioned purposes or as required by law; (iii) sell Customer Personal Data; (iv) retain, use, or disclose Customer Personal Data outside of the direct business relationship between Kyriba and Customer. Kyriba certifies that it understands these restrictions and will comply with them. If Kyriba must process Customer Personal Data as otherwise required by applicable law, Kyriba shall inform Customer of that legal requirement before processing Customer Personal Data, unless that law prohibits such disclosure on important grounds of public interest. Notwithstanding the above, to the extent any Customer Personal Data becomes “deidentified” or in the “aggregate” as those terms are defined under Applicable Data Protection Law, Kyriba may use such information for any commercial purpose in accordance with Applicable Data Protection Law, including but not limited to developing analytics, and may retain, use and disclose such information for such purpose, without restriction. The purpose and duration of the processing, its nature, the type of Customer Personal Data subject to processing and the categories of data subjects are specified in the Data Protection Schedule attached hereto and incorporated by reference herein.

3. In the event Customer Personal Data relates to EU data subjects, Kyriba will comply with the requirements set forth in Article 28 of the GDPR and the description of processing in the Data Protection Schedule attached hereto. Accordingly, Kyriba shall (i) ensure that Kyriba employees authorized to process Customer Personal Data under this Addendum are bound by confidentiality terms substantially similar to those of the Agreement or the appropriate statutory obligation of confidentiality, (ii) taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, maintain reasonable security measures and appropriate technical and organizational measures referred to in Article 32 of the GDPR for the protection, confidentiality, and integrity of Customer Personal Data, (iii) regularly monitor compliance with these measures, and shall not materially decrease the overall security of the SaaS Services during its provision of the SaaS Services pursuant to the Agreement, (iv) to the extent legally permitted, promptly notify Customer if Kyriba receives a request from an individual, consumer, or data subject to exercise their rights under Applicable Data Protection Law or receives a request or complaint from a supervisory authority or other third party (“**Request**”), (v) taking into account the nature of the

processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising the individual, consumer, or data subject's rights, and shall not respond to such Requests without written approval from Customer, except as necessary to comply with Applicable Data Protection Law, (vi) upon Customer's written request, and subject to Section 6.3 (Customer Data) of the Agreement, delete or return all Customer Personal Data to Customer within sixty (60) days after termination of the Agreement for any reason or if Customer Personal Data is no longer needed to perform the SaaS Services; however, Kyriba may retain Customer Personal Data where necessary for Kyriba to comply with applicable law or legal obligation, or its rights or those of a third party, and (vii) make available to Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in this Section and allow for, to the extent required by law, contribution to audits, including inspections, conducted by Customer or another auditor mandated by Customer. Such auditor will have to be bound by confidentiality undertakings at least as stringent as those set out in the Agreement. To the extent legally permitted, Customer shall be responsible for any costs arising from Kyriba's provision of assistance hereunder.

4. Kyriba uses sub-processors to carry out specific processing activities, such as hosting or maintenance. Sub-processors used as at the date of the present addendum are specified in the Data Protection Schedule attached hereto. In addition, Customer provides general written authorization to Kyriba to engage another sub-processor in connection with Customer's use of the SaaS Services. If Kyriba wishes to replace one of its existing sub-processors or hire a new sub-processor ("**Change**"), Kyriba will inform Customer in advance of any proposed changes in connection with Customer's use of the SaaS Services; thereby giving Customer the opportunity to object to such Change. Customer has a maximum period of two (2) business days from the date of receipt of this information to expressly object to the Change on reasonable grounds by sending a notice to Kyriba. Such notice shall set out the reasons for such objection. In the event Customer sends a notice objecting to the new sub-processor, the parties will seek to resolve the issue through a mutually agreeable understanding. Kyriba will use commercially reasonable efforts to make available to Customer a change in the SaaS Services or Customer's configuration thereof to avoid the processing of Customer Personal Data by the objected-to new sub-processor. If five (5) days before the effective date of the Change, the parties have failed to reach a common understanding, Customer will be entitled to terminate the Agreement with effect as at the effective date of the Change. If Customer does not terminate the Agreement pursuant to this Section, Customer will be considered as having agreed to the Change. This termination right is Customer's sole and exclusive remedy if Customer objects to any new sub-processor. Kyriba will sign a written agreement with any sub-processor it engages to ensure that such sub-processor complies with the provisions of this Section and meets the requirements laid down in the Applicable Data Protection Law. Kyriba will remain responsible and liable for the compliance by any such sub-processor with the terms of this Section.

5. Customer is solely responsible for the accuracy, quality, and legality of Customer Personal Data. Customer represents and warrants to Kyriba that, in respect of all Customer Personal Data, Customer has the necessary authority, license or consent to provide Customer Personal Data and has a lawful basis (including all legally required notices and consents), has complied (and will continue to comply) with all Applicable Data Protection Law, in particular for the sharing, transmission, and processing of Customer Personal Data with, to, and by Kyriba for the purposes of the SaaS Services and the Agreement, and Kyriba's processing of Customer Personal Data in accordance with Customer's instructions will not cause Kyriba to violate any Applicable Data Protection Law.

6. Customer acknowledges and agrees that Customer Personal Data may be transferred outside European Union countries to countries recognized by the European Commission as countries where there is an adequate level of protection as updated from time to time ("**Authorized Location**"). During the term of the Agreement, Kyriba shall be Privacy Shield certified. In the event Customer agrees to a transfer of Customer Personal Data outside an Authorized Location, such transfer shall be subject to the execution between the Parties of the EU Standard Contractual Clauses or any other alternative mean validated by GDPR.

7. Kyriba maintains security incident management policies and procedures, and upon occurrence of any actual security breach affecting Customer Personal Data

transmitted, stored, or otherwise processed by Kyriba, (the “**Information Security Breach**”), Kyriba shall:

- (i) notify Customer, within 72 hours of confirmation of, and without undue delay, the Information Security Breach, and deliver to Customer a written report regarding the nature of the Information Security Breach, the categories and the approximate number of Customer Personal Data affected, if such information is available. Kyriba shall also describe the likely consequences of the Information Security Breach on Customer Personal Data as well as the reasonable measures Kyriba deems necessary and reasonable to remediate the cause of such Information Security Breach, to the extent the remediation is within Kyriba’s reasonable control, including, where appropriate, to mitigate its possible adverse effects; and
- (ii) Proceed as quickly as reasonably possible (a) to mitigate any adverse impact or other harm to Customer and any affected individuals, consumers, and data subjects resulting from such Information Security Breach; and (b) to prevent similar Information Security Breaches from occurring in the future. Kyriba will keep Customer fully informed of all stages of its investigation and all actions taken as a result thereof.

This Addendum shall be effective as of the effective date of the Agreement and shall remain effective for so long as the Agreement remains in effect. Only a written agreement signed by authorized representatives of both parties can modify this Addendum. In the event of inconsistency between the Agreement and the Addendum provisions, the parties agree that the provisions of this Addendum will prevail.

Executed by **Kyriba Corp.**

Executed by **CUSTOMER:** _____

Authorized Signature:

Authorized Signature:

Name _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

ATTACHMENT 1 TO THE ADDENDUM: DATA PROTECTION SCHEDULE

This Data Processing Schedule is part of the Addendum and of the Agreement and details the characteristics of processing Customer Personal Data.

1. Description of processing

Type of Customer Personal Data	Categories of individuals, consumers, or data subject	Purpose of processing	Duration of processing	
Determined and controlled by Customer, in Customer's discretion; and may include, without limitation, name, email address, phone number, IP address, Ad ID, username and password, government issued identification, and financial accounts	Customer's employees, representatives, contractors, partners, vendors, persons of interest, and/or customers	Provision of SaaS Services under the Agreement	Duration of the processing shall correspond to the duration of the Agreement except where otherwise required by applicable law or legal obligation, or for Kyriba to protect its rights or those of a third party.	

2. Subprocessors

Affiliates of Kyriba (for purposes of implementation, support and maintenance)

FireEye, Inc. DBA Mandiant (if the event of a data breach, for purposes of data breach investigation and remediation)

Amazon Web Services, Inc. (for purposes of providing infrastructure for Kyriba's application)

Iron Mountain Incorporated (for purposes of providing infrastructure for Kyriba's application)

Equinix (France) SAS (for purposes of providing infrastructure for Kyriba's application)

Sage Intacct, Inc. (for purposes of invoice generation and management)

Salesforce.com, Inc. (for administration of contract)

Salesforce.com EMEA Limited (for administration of contract)

Digital Guardian, Inc. (for data loss prevention and monitoring)

Netskope, Inc. (in the event of data breach, provides data loss prevention solution)

Mimecast North America, Inc. (provides email security tool to protect Kyriba against spam, viruses and malware)

Splunk, Inc. (provides security analytics tool to identify anomalous activity within Kyriba's environment)

SIA S.P.A. (provides connection to Italian banking protocol)

Fujitsu FIP Corporation (provides connection to Japanese banking protocol)

ServiceNow, Inc. (provides tool to ticket, track and process customer support requests)

It is understood that Kyriba may change, substitute or add subprocessors in accordance with Section 4 of the Addendum.