POSIT SOFTWARE, PBC
DATA PROCESSING ADDENDUM
Last Updated: March 15, 2023

This Data Processing Addendum, including its Schedules, ("DPA") forms part of the Posit Service Terms of Use or other written or electronic agreement between Posit Software, PBC ("Posit") and the Customer for the access and use of Posit's software as a service solutions (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") (the "Agreement") to reflect the Parties' agreement with regard to the Processing of Personal Data.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates (if any). All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In the course of providing the Services to Customer pursuant to the Agreement, Posit may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

Except as otherwise expressly provided in the Agreement, this DPA will become legally binding upon execution by a duly authorized representative of both Posit and Customer.

For the avoidance of doubt, signature of the DPA shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses, including Schedule 2. Where Customer wishes to separately execute the Standard Contractual Clauses and its Appendix, Customer should also complete the information as the data exporter and sign Schedule 2.

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement.

If the Customer entity signing this DPA has executed an Order Form with Posit for Services pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form for Services and applicable renewal Order Form for Services.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Order Form or Agreement executes this DPA.

In the event of a conflict between this DPA and the Agreement in connection with terms and conditions relating to Processing of Customer Data, this DPA will take precedence over the Agreement.

If the Customer entity signing the DPA is not a party to an Order Form nor an Agreement directly with Posit, but is instead a customer indirectly via an authorized reseller of Posit services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

DATA PROCESSING TERMS

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% ofthe voting interests of the subject entity.

"**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Posit, but hasnot signed its own order with Posit and is not a "Customer" as defined under this DPA.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Customer**" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms.

"Customer Data" means electronic data and information submitted by or for Customer to the Services.

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement as amended from time to time.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"**Europe**" means the European Union, the European Economic Area, Switzerland and the United Kingdom.

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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), including as implemented or adopted under the lawsof the United Kingdom.

"Personal Data" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as Personal Data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

"Processing" or **"Process"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

"**Public Authority**" means a government agency or law enforcement authority, including judicial authorities.

"Standard Contractual Clauses" means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

"Sub-processor" means any Processor engaged by Posit.

2. PROCESSING OF PERSONAL DATA

2.1. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Posit is the Processor and that Posit will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2. **Customer's Processing of Personal Data.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of Posit as Processor. For the avoidance of doubt, Customer's instructions to Posit for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject, including those that have opted-out from sales or other disclosures of Personal Data, to the extent applicable under Data Protection Laws and Regulations.

2.3. **Posit's Processing of Personal Data.** Posit shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions and Customer's use of the Services for the following purposes:
(i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.4. **Details of the Processing.** The subject-matter of Processing of Personal Data by Posit is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Description of Processing/Transfer) to this DPA.

3. RIGHTS OF DATA SUBJECTS

Posit shall, to the extent legally permitted, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject such as a Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decisionmaking, each such request being a "Data Subject Request". Posit shall not respond to a Data Subject Request itself, except that Customer authorizes Posit to redirect the Data Subject Request as necessary to allow Customer to respond directly. Taking into account the nature of the Processing, Posit shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Posit shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Posit is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Posit's provision ofsuch assistance.

4. POSIT PERSONNEL

4.1. **Confidentiality.** Posit shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Posit shall ensure that such confidentiality obligations survive the termination of the personnel engagement, to the extent set forth in the Agreement.

4.2. **Reliability.** Posit shall take commercially reasonable steps to ensure the reliability of any Posit personnel engaged in the Processing of Personal Data.

4.3. **Limitation of Access.** Posit shall ensure that Posit's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. SUB-PROCESSORS

5.1. **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Posit's Affiliates may be retained as Sub-processors; and (b) Posit may engage third-party Sub-processors in connection with the provision of the Services. Posit has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the

protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2. **List of Current Sub-processors and Notification of New Sub-processors.** The current list of Sub-processors engaged inProcessing Personal Data for the performance of the Service, including a description of their processing activities and countries of location, is set forth in Schedule 3. Customer hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data.

5.3. **Objection Right for New Sub-processors.** Prior to retaining or engaging a new Sub-processor, Posit shall provide written notice to Customer by email of Posit's intent to retain or engage a new Sub-processor; such notice shall include the identity of such new Sub-processor, their country of location and the duties of such new Sub-processor with respect to Personal Data ("**Notice of New Sub-processor**"). Customer may object to Posit's use of a new Sub-processor by notifying Posit promptly in writing within thirty (30) days after receipt of Posit's notice (the "**Objection Period**"). In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Posit will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Posit is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Posit without the use of the objected-to new Sub-processor by providing written notice to Posit. **IF SUBSCRIBER DOES NOT OBJECT IN WRITING TO A NOTICE OF NEW SUB-PROCESSOR PRIOR TO THE EXPIRATION OF THE APPLICABLE OBJECTION PERIOD, THEN SUBSCRIBER WILL BE DEEMED TO HAVE CONSENTED TO AND ACCEPTED POSIT'S ENGAGEMENT OF THE NEW SUB-PROCESSOR AS SET FORTH IN SUCH NOTICE OF NEW SUB-PROCESSOR.** Posit will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4. **Liability.** Posit shall be liable for the acts and omissions of its Sub-processors to the same extent Posit would be liable if performing the services of each Sub-processor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

6. SECURITY

6.1. **Controls for the Protection of Customer Data.** Customer maintains ownership of and control over all Customer Data. Customer grants limited rights to Process Customer Data within the Customer account but Customer maintains full control and authority of all Processed Customer Data. Posit shall maintain appropriate technical and organizational measures for protection of the security of Customer Data (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data) within Posit's control, and the confidentiality and integrity of Customer Data within Posit's control. Posit regularly monitors compliance with these measures. Posit will not materially decrease the overall security of the Services during a subscription term.

6.2. **Audit.** Posit shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to Customer information to demonstrate compliance with the obligations set out in this DPA as set forth in this section 6.2.

6.2.1. Third-Party Certifications and Audits. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Posit shall make available to Customer (or Customer's Third-Party Auditor - as defined below in section 6.2.4) information regarding Posit's compliance with the obligations set forth in this DPA in the form of a copy of Posit's then most recent third-party audits or certifications. Such third-party audits or certifications may also be shared with Customer's competent supervisory authority on its request. Where Posit has obtained ISO 27001 certifications and SSAE 18 Service Organization Control (SOC) 2 reports for the Services, Posit agrees to maintain these certifications or standards, or appropriate and comparable successors thereof, for the duration of the Agreement. Upon request, Posit shall also provide a requesting Customer with a report and/or confirmation of Posit's audits of third party Sub-processors' compliance with the data protection controls set forth in this DPA and/or a report of third-party auditors' audits of third-party Sub-processors that have been provided by those third-party Sub-processors to Posit, to the extent such reports or evidence

may be shared with Customer ("Third-party Sub-processor Audit Reports"). Customer acknowledges that (i) Third-party Sub-processor Audit Reports shall be considered Confidential Information as well as confidential information of the third-party Sub-processor and (ii) certain third-party Sub-processors to Posit may require Customer to execute a non-disclosure agreement with them in order to view a Third-party Sub-processor Audit Report.

6.2.2. On-Site Audit. Customer may contact Posit to request an on-site audit of Posit's Processing activities covered bythis DPA ("On-Site Audit"). An On-Site Audit may be conducted by Customer either itself or through a Third-Party Auditor (as defined below in section 6.2.4) selected by Customer when:

(i) the information available pursuant to section "Third-Party Certifications and Audits" is not sufficient to demonstratecompliance with the obligations set out in this DPA and its Schedules;
(ii) Customer has received a notice from Posit of a Customer Data Incident; or
(iii) such an audit is required by Data Protection Laws and Regulations or by Customer's competent supervisory authority.

Any On-Site Audits will be limited to Customer Data Processing and storage facilities operated by Posit or any of Posit's Affiliates. Customer acknowledges that Posit operates a multi-tenant cloud environment. Accordingly, Posit shall have the right to reasonably adapt the scope of any On-Site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Posit customers' information.

6.2.3. Reasonable Exercise of Rights. An On-Site Audit shall be conducted by Customer or its Third-Party Auditor:

(i) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of theServices used by Customer;
(ii) up to one time per year with at least three weeks' advance written notice. If an emergency justifies a shorter noticeperiod, Posit will use good faith efforts to accommodate the On-Site Audit request; and
(iii) during Posit's normal business hours, with a representative of Posit present, under reasonable duration and shall not unreasonably interfere with Posit'sday-to-day operations.

Before any On-Site Audit commences, Customer and Posit shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of Posit.

6.2.4. Third-Party Auditor. A Third Party Auditor means a third-party independent contractor that is not a competitor of Posit. An On-Site Audit can be conducted through a Third Party Auditor if:

(i) prior to the On-Site Audit, the Third Party Auditor enters into a non-disclosure agreement containing confidentialityprovisions no less protective than those set forth in the Agreement to protect Posit's proprietary information; and
(ii) the costs of the Third Party Auditor are at Customer's expense.

6.2.5. Findings. Customer must promptly provide Posit with information regarding any non-compliance discovered during the course of an On-Site Audit, all of which are deemed Posit's Confidential Information.

6.3. Data Protection Impact Assessment. Upon Customer's request, Posit shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Data Protection Laws and Regulations to carry outa data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Posit.

7. SUBSCRIBER DATA INCIDENT MANAGEMENT AND NOTIFICATION

Posit maintains security incident management policies and procedures and shall, notify Customer without undue delay, and, where feasible, not later than 72 hours, after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Posit or its Sub-processors of which Posit becomes aware (a "Customer Data Incident"). Posit shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Posit deems necessary and reasonable to remediate the cause of such a Customer Data Incident to the extent the remediation is within Posit's reasonable

control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

8. GOVERNMENT ACCESS REQUESTS

8.1 Posit requirements. In its role as a Processor, Posit shall maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including by implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense and public security. If Posit receives a legally binding request to access Personal Data from a Public Authority, Posit shall, unless otherwise legally prohibited, promptly notify Customer including a summary of the nature of the request. To the extent Posit is prohibited by law from providing such notification, Posit shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Posit to communicate as much information as possible, as soon as possible. Further, Posit shall challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. Posit shall pursue possibilities of appeal. When challenging a request, Posit shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. Posit agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. Posit shall promptly notify Customer if Posit becomes aware of any direct access by a Public Authority to Personal Data and provide information available to Posit in this respect, to the extent permitted by law. For the avoidanceof doubt, this DPA shall not require Posit to pursue action or inaction that could result in civil or criminal penalty for Posit such as contempt of court.

8.2 Sub-processors requirements. Posit shall ensure that Sub-processors involved in the Processing of Personal Data aresubject to the relevant commitments regarding Government Access Requests in the Standard Contractual Clauses.

9. RETURN AND DELETION OF SUBSCRIBER DATA

Upon termination or expiration of the Agreement, Posit shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with Posit's standard data retention policies. Until Customer Data is deleted or returned, Posit shall continue to comply with this DPA and its Schedules.

10. AUTHORIZED AFFILIATES

10.1. Contractual Relationship. The parties acknowledge and agree that, by executing the Agreement, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishinga separate DPA between Posit and each such Authorized Affiliate subject to the provisions of the Agreement and this DPA. Each Authorized Affiliate agrees to be bound by the obligations set forth in this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a partyto the Agreement, and is a party only to this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions ofthe Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

10.2. Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinatingall communication with Posit under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10.3. Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to this DPA with Posit, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remediesunder this DPA, subject to the following:

10.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Posit directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting

party to the Agreement shall exercise any such rights under this DPA, not separately for each Authorized Affiliate individually, but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in section 10.3.2, below).

10.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an On-Site Audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Posit and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

11. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Posit, whether in contract, tort or under any other theory of liability, is subject tothe 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, Posit's total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate thatis a contractual party to any such DPA.

12. EUROPE SPECIFIC PROVISIONS

12.1. Definitions. For the purposes of this section 12 and Schedule 1 these terms shall be defined as follows:

"EU C-to-P Transfer Clauses" means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extentthey reference Module Two (Controller-to-Processor).

"EU P-to-P Transfer Clauses" means Standard Contractual Clauses sections I, II III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor).

12.2. GDPR. Posit will Process Personal Data in accordance with the GDPR requirements directly applicable to Posit's provision of its Services.

12.3. Customer Instructions. Posit shall inform Customer without undue delay (i) if, in its opinion, an instruction from Customer constitutes a breach of the GDPR and/or (ii) if Posit is unable to follow Customer's instructions for the Processing of Personal Data.

12.4. Transfer mechanisms for data transfers. If, in the performance of the Services, Personal Data that is subject to the GDPR or any other law relating to the protection or privacy of individuals that applies in Europe is transferred out of Europe to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations of Europe, the transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the Parties to the extent such transfers are subject to the Data Protection Laws and Regulations of Europe:

- **The EU C-to-P Transfer Clauses**. Where Customer and/or its Authorized Affiliate is a Controller and a data exporter of Personal Data and Posit is a Processor and data importer in respect of that Personal Data, then the Parties shall comply with the EU C-to-P Transfer Clauses, subject to the additional terms in section 2 of Schedule 1; and/or

- **The EU P-to-P Transfer Clauses**. Where Customer and/or its Authorized Affiliate is a Processor acting on behalf of a Controller and a data exporter of Personal Data and Posit is a Processor and data importer in respect of that Personal Data, the Parties shall comply with the terms of the EU P-to-P Transfer Clauses, subjectto the additional terms in sections 2 and 3 of Schedule 1.

12.5. Impact of local laws. As of the Effective Date, Posit has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Personal Data as set forth in the

Infrastructure and Sub-processorsDocumentation, including any requirements to disclose Personal Data or measures authorizing access by a Public Authority, prevent Posit from fulfilling its obligations under this DPA. If Posit reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of the Personal Data ("Local Laws") prevent it from fulfilling its obligations under this DPA, it shall promptly notify Customer. In such a case, Posit shall use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to facilitate compliance with the Local Laws without unreasonably burdening Customer. If Posit is unable to make available such change promptly, Customer may terminate the applicable Order Form(s) and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by Posit in accordance with the Local Laws by providing written notice in accordance with the "Notices" section of the Agreement. Customer shall receive a refund of any prepaid fees for the periodfollowing the effective date of termination for such terminated Services.

13. CALIFORNIA CONSUMER PRIVACY ACT OF 2018

Posit agrees that Customer discloses Personal Data to Posit solely (i) for a valid business purpose; and (ii) to allow Posit to perform the Services. Posit shall not: (i) sell (or, effective January 1, 2023, share) Personal Data as the terms sell and share are defined under Data Privacy Laws; (ii) retain, use, or disclose Personal Date for any purpose other than for the specific purpose of performing the Services; (iii) retain, use, or disclose Personal Date for a commercial purpose other than providing the Services pursuant to the Agreement; (iv) retain, use, or disclose Personal Date outside of the direct business relationship between the parties; or (e) effective January 1, 2023, combine Personal Date that Posit receives with Personal Information that Posit receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that Posit may combine such information to perform any business purpose as defined under Data Privacy Laws. Posit understands the prohibitions and requirements set forth in this Section 13 and will comply with them.

14. LEGAL EFFECT

This DPA shall only become legally binding between Customer and Posit when a duly authorized representative of each party has executed this DPA.

List of Schedules

Schedule 1: Transfer Mechanisms for European Data Transfers

Schedule 2: Description of Processing/Transfer

IN WITNESS WHEREOF, the parties' authorized signatories have duly executed this DPA:

POSIT SOFTWARE, PBC	**CUSTOMER**
By: _____	**By:** _____
Name: Tareef Kawaf	**Name:**
Title: President	**Title:**
Date: Mar 28, 2023	**Date:**

SCHEDULE 1 - TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

1. STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS

1.1. For the purposes of the EU C-to-P Transfer Clauses and the EU P-to-P Transfer Clauses, Customer is the data exporter and Customer is the data importer and the Parties agree to the following. If and to the extent an Authorized Affiliate relieson the EU C-to-P Transfer Clauses or the EU P-to-P Transfer Clauses for the transfer of Personal Data, any references to "Customer" in this Schedule, include such Authorized Affiliate. Where this section 2 does not explicitly mention EU C-to-P Transfer Clauses or EU P-to-P Transfer Clauses it applies to both of them.

1.2. **Reference to the Standard Contractual Clauses.** The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 2.

1.3. **Docking clause.** The option under clause 7 shall not apply.

1.4. **Instructions.** This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to Posit for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Customer to Process Personal Data are set out in section 2.3 of this DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.

1.5. **Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Posit to Customer only upon Customer's written request.

1.6. **Security of Processing.** For the purposes of clause 8.6(a), Customer is solely responsible for making an independent determination as to whether the technical and organizational measures maintained by Posit meet Customer's requirements and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by Posit provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with section 7 (Customer Data Incident Management and Notification) of this DPA.

1.7. **Audits of the SCCs.** The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with section 6.2 of this DPA.

1.8. **General authorization for use of Sub-processors.** Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Posit has Customer's general authorization to engage Sub-processors in accordance with section 5 of this DPA. Posit shall make available to Customer the current list of Sub-processors in accordance with section 5.2 of this DPA. Where Posit enters into the EU P-to-P Transfer Clauses with a Sub-processor in connection with the provision of the Services, Customer hereby grants Posit and Posit's Affiliates authority to provide a general authorization on Controller's behalf for the engagement of sub-processors by Sub-processors engaged in the provision of the Services, as well as decision making and approval authority for the addition or replacement of any such sub-processors.

1.9. **Notification of New Sub-processors and Objection Right for new Sub-processors.** Pursuant to clause 9(a), Customer acknowledges and expressly agrees that Posit may engage new Sub-processors as described in sections 5.2 and 5.3 of this DPA. Posit shall inform Customer of any changes to Sub-processors following the procedure provided for in section 5.2 of this DPA.

1.10. **Complaints - Redress.** For the purposes of clause 11, and subject to section 3 of this DPA, Posit shall inform data subjects on its website of a contact point authorized to handle complaints. Posit shall

inform Customer if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Customer. Posit shall not otherwise have any obligation to handle the request (unless otherwise agreed with Customer). The option under clause 11 shall not apply.

1.11. **Liability.** Posit's liability under clause 12(b) shall be limited to any damage caused by its Processing where Posit has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Customer, as specified in Article 82 GDPR.

1.12. **Supervision.** Clause 13 shall apply as follows:

1.12.1. Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

1.12.2. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuantto Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

1.12.3. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, DO2 RD28, Ireland shall act as competent supervisory authority.

1.12.4. Where Customer is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as competent supervisory authority.

1.12.5. Where Customer is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

1.13. **Notification of Government Access Requests.** For the purposes of clause 15(1)(a), Posit shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

1.14. **Governing Law.** The governing law for the purposes of clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of Republic of Ireland; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.

1.15. **Choice of forum and jurisdiction.** The courts under clause 18 shall be those designated in the Venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) Republic of Ireland; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

1.16. **Appendix.** The Appendix shall be completed as follows:

- The contents of section 1 of Schedule 2 shall form Annex I.A to the Standard Contractual Clauses
- The contents of sections 2 to 9 of Schedule 2 shall form Annex I.B to the Standard Contractual Clauses
- The contents of section 10 of Schedule 2 shall form Annex I.C to the Standard Contractual Clauses
- The contents of section 11 of Schedule 2 to this Exhibit shall form Annex II to the Standard Contractual Clauses.

1.17. **Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses.** In case of any transfers of Personal Data from the United Kingdom and/or transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Data Protection Laws and Regulations of the United Kingdom ("UK Data Protection Laws") or Swiss Data Protection Laws, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection Laws, as applicable. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

1.18. **Conflict.** The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

2. ADDITIONAL TERMS FOR THE EU P-TO-P TRANSFER CLAUSES

For the purposes of the EU P-to-P Transfer Clauses (only), the Parties agree the following.

2.1. **Instructions and notifications.** For the purposes of clause 8.1(a), Customer hereby informs Posit that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data. Customer warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Posit for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant Controller. Customer shall be solely responsible for forwarding any notifications received from Posit to the relevant Controller where appropriate.

2.2. **Security of Processing.** For the purposes of clause 8.6(c) and (d), Posit shall provide notification of a personal data breach concerning Personal Data Processed by Posit to Customer.

2.3. **Documentation and Compliance.** For the purposes of clause 8.9, all enquiries from the relevant Controller shall be provided to Posit by Customer. If Posit receives an enquiry directly from a Controller, it shall forward the enquiry to Customer and Customer shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.

2.4. **Data Subject Rights**. For the purposes of clause 10 and subject to section 3 of this DPA, Posit shall notify Customer about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Customer shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

SCHEDULE 2 - DESCRIPTION OF PROCESSING/TRANSFER

1. LIST OF PARTIES

Data exporter: *Identity and contact details of the data exporter and, where applicable, of their data protection officer and/or representative in the European Union*

Customer Name:	
Customer Address:	
Contact person's name, position and contact details:	
Notification email address:	
Activities relevant to the data transferred under these clauses:	Performance of the Services pursuant to the Agreement and as further described in the Documentation.
Role:	For the purposes of the EU C-to-P Transfer Clauses Customer and/or its Authorized Affiliate is a Controller. For the purposes of the EU P-to-P Transfer Clauses Customer and/or its Authorized Affiliate is a Processor.
Signature and date:	

Data importer: *Identity and contact details of the data importer, including any contact person with responsibility for data protection.*

Name:	Posit Software, PBC
Address:	250 Northern Avenue, Boston, MA 02210
Contact person's name, position and contact details:	Information Operations (attn: Privacy) privacy@posit.co
Activities relevant to the data transferred under these clauses:	Performance of the Services pursuant to the Agreement and as further described in the Documentation.
Role:	Processor
Signature and date:	 Mar 28, 2023

2. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its solediscretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customer employees, contractors, agents, and/or representatives who are assigned accounts on the Services.

3. CATEGORIES OF PERSONAL DATA TRANSFERRED

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Corporate contact information such as name, job title, email address, physical address, phone number, and localization data.

SCHEDULE 3 - STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

1. For the purposes of Article 26(2) of Directive 95/46/EC SENSITIVE DATA TRANSFERRED (IF APPLICABLE)

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of thedata and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

None. No sensitive data transfer is authorized.

2. FREQUENCY OF THE TRANSFER

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous basis depending on the use of the Services by Customer.

3. NATURE OF THE PROCESSING

The nature of the Processing is the performance of the Services pursuant to the Agreement.

4. PURPOSE OF PROCESSING, THE DATA TRANSFER AND FURTHER PROCESSING

Posit will Process Personal Data as necessary to perform the Services pursuant to the Agreement, and as further instructed by Customer in its use of the Services.

5. DURATION OF PROCESSING

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Subject to section 9 of the DPA, Posit will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

6. SUB-PROCESSOR TRANSFERS

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

As per 7 above, the Sub-processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement. Subject to section 9 of this DPA, the Sub-processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Identities of the Sub-processors used for the provision of the Services and their country of location as follows:

Sub-Processor	Type of Service	Hosting Region	EU & UK Data Transfer Mechanism
Amazon Web Services	Cloud Computing Provider	United States	SCC
Chargify	Subscription Management (if payment made by credit card)	United States	SCC
Datadog	Centralized Logging	United States	SCC
Mailgun Technologies	Email Notification Services	United States	SCC
Oracle (NetSuite)	Billing Provider	United States	SCC
Salesforce	Customer Relationship Management	United States	SCC
Stripe	Payment Processing (if payment made by credit card)	United States	SCC
Zendesk	Customer Support Case Management	United States	SCC

7. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with clause 13:

a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility forensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

b. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as the competent supervisory authority.

c. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: the Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, DO2 RD28, Ireland shall act as the competent supervisory authority.

d. Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as the competent supervisory authority.

e. Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

8. TECHNICAL AND ORGANISATIONAL MEASURES

Data importer will maintain administrative, physical, and technical safeguards designed for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services and will not materially decrease the overall security of the Services during a subscription term. Data Subject Requests shall be handled in accordance with section 3 of the DPA.

An overview of Posit's data protection practices are as follows:

a. **Information Security Program**. The Posit Information Security Program designed to maintain the confidentiality, integrity and availability of its information systems while meeting necessary legal and contractual requirements. The information security program includes technical and organizational security measures as well as policies and procedures to protect data processed by Posit.

b. **Logical Access Controls.** Policies and procedures governing the granting of access ensure that only authorized users can grant, modify or revoke access to Information systems housing customer data. Authorized users are assigned unique user-IDs and required to follow secure password policy and use multi-factor authentication where appropriate.

   Access rights are provisioned adhering to the "least privilege" approach, granting only those rights to users as may be required to perform their assigned duties. Such rights are reviewed regularly and revoked when no longer appropriate.

c. **Systems & Data Security Controls.** Posit shall maintain policies and procedures to ensure that system, application and infrastructure development is performed in a secure manner. This includes review and testing of products and services for common security vulnerabilities and defects, employing defense-in-depth strategy, periodic penetration testing and security assessment of these services.

   Access to the service and electronic transmission of data uses industry-standard encryption protocols such as Transport Layer Security (TLS). Databases are encrypted at rest. Posit will maintain corrective action and incident response plans to respond to potential security threats.

d. **Physical Access Controls.** Sub-processor data centers have appropriate security protections in place to guard against unauthorized physical access to such facilities. Protections include access control, video surveillance, security personnel, and intrusion detection systems. Physical access to data centers is restricted to those having legitimate business needs and is controlled and logged using appropriate access and authentication technologies and practices.

e. **Vulnerability Management.** At least quarterly, Posit scans system source code with industry-standard vulnerability scanning software to detect source code vulnerabilities. Posit undergoes third-party penetration testing of its cloud services on an annual basis. Any vulnerabilities found during this testing will be remediated in accordance with Posit's vulnerability management policies and procedures and will be assessed based on Posit's risk management framework.

f. **Continued Evaluation.** Posit will conduct periodic reviews of the security of the Posit systems and adequacy of its information security program as measured against industry security standards and its policies and procedures. Posit will continually evaluate the security of its systems and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.