



SAS DATA PROCESSING ADDENDUM FOR CUSTOMERS

This Data Processing Addendum (“**Addendum**”) supplements any binding, written agreement between Customer and SAS that specifically incorporates its terms by reference (“**Agreement**”), and will apply to the extent that SAS or a SAS Affiliate processes Personal Data on Customer’s behalf pursuant to the Agreement.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

1. **Definitions.** Any capitalized terms used in this Addendum that are not defined below have the meanings set forth in the Agreement.
 - 1.1. “**Applicable Data Protection Laws**” means all laws and regulations, including the laws of the EEA, Switzerland, the United Kingdom (“**UK**”), and the United States and its states, that are applicable to the Processing of Personal Data under the Agreement, as amended from time to time.
 - 1.2. “**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data.
 - 1.3. “**Customer**” means the Customer and any of Customer’s Related Entities that are permitted to receive or use the Services performed by SAS under the Agreement.
 - 1.4. “**Data Subject**” means the natural person to whom Personal Data relates.
 - 1.5. “**Data Subject Request**” means a request from a Data Subject to access, delete, release, correct or block access to specific Personal Data or otherwise to exercise rights provided under Applicable Data Protection Laws.
 - 1.6. “**EEA**” means the Member States of the European Union, as well as Iceland, Liechtenstein, and Norway.
 - 1.7. “**EEA Restricted Transfer**” means a transfer (or onward transfer) to a Third Country of Personal Data originating in the EEA or Switzerland that is subject to GDPR or the Swiss Federal Act on Data Protection, where any required adequacy means can be met by entering into the EU Standard Contractual Clauses.
 - 1.8. “**EU Standard Contractual Clauses**” means the standard contractual clauses annexed to Commission Implementing Decision (EU) (2021/914) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. This term also includes any subsequent version thereof released by the European Commission. In the event any subsequent version of such clauses is released that is applicable to the Services, the parties agree that the then-current version of the clauses will apply, in which case any references in this Addendum to specific clauses in the clauses shall be deemed to refer to equivalent clauses in the then-current version of the clauses, regardless of their enumeration.
 - 1.9. “**GDPR**” means Regulation 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 the Free Movement of Such Data, repealing Directive 95/46/EC, otherwise known as the General Data Protection Regulation, and for the purpose of this Addendum includes the corresponding laws of the UK (including the UK GDPR and Data Protection Act 2018).
 - 1.10. “**Personal Data**” means any information relating to an identified or identifiable natural person, including without limitation any information protected as “personal data” or “personal information” under Applicable Data Protection Laws, that is included in the Customer Materials and that SAS processes on behalf of Customer in the course of providing the Services to Customer.

- 1.11. **“Processing”** 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.
- 1.12. **“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 Applicable Data Protection Laws.
- 1.13. **“Related Entity”** shall have the meaning set forth in the Agreement.
- 1.14. **“SAS”** means the SAS entity that is party to the Agreement.
- 1.15. **“SAS Affiliate”** means any SAS entity that is not party to the Agreement, including as applicable SAS Institute Inc. if it is not party to the Agreement, and any direct or indirect subsidiary of SAS Institute Inc. that is not party to the Agreement.
- 1.16. **“Security Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data while such data is being Processed by SAS under the Agreement.
- 1.17. **“Services”** means SAS’ performance of its obligations that require Processing of Personal Data under the Agreement.
- 1.18. **“Subprocessors”** means SAS Affiliates and/or any third-party subcontractors who have been engaged by SAS to Process Personal Data in connection with the Services.
- 1.19. **“Term”** means the period during which SAS will perform the Services under the Agreement.
- 1.20. **“Third Country”** means any country, organization, or territory not acknowledged by the European Commission or the UK government, as applicable, to ensure an adequate level of protection for Personal Data in accordance with Article 45 of GDPR.
- 1.21. **“UK Addendum”** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, issued by the UK Information Commissioner’s Office under S119A(1) Data Protection Act 2018 and in force as of 21 March 2022, as revised by the UK Information Commissioner’s Office from time to time.
- 1.22. **“UK Restricted Transfer”** means a transfer (or onward transfer) to a Third Country of Personal Data originating in the UK that is subject to GDPR where any required adequacy means can be met by entering into the EU Standard Contractual Clauses and the UK Addendum.

2. Roles of the Parties; Details of the Processing.

- 2.1. Roles of the Parties. Customer and/or its Related Entities are the Controller(s) of the Personal Data, except where Customer and/or its Related Entities act as Processor(s) for another Controller, in which case they shall in relation to SAS exercise the rights and obligations of the applicable Controller under this Addendum. SAS is a Processor of the Personal Data.
- 2.2. Details of the Processing. Schedule 1 specifies the details of the Processing, including the subject matter, nature, duration and purposes of the Processing, the types of Personal Data and the categories of Data Subjects.

3. Customer Obligations as Controller.

Customer is responsible for complying with its obligations as a Controller under Applicable Data Protection Laws. To that end, Customer must: (a) justify any transmission of Personal Data to and Processing of Personal Data by SAS (including where applicable providing any notices and obtaining any consents required by Applicable Data Protection Laws), and (b) be responsible for its decisions and actions concerning the Processing and use of Personal Data, including Customer’s instructions to SAS regarding the Processing of Personal Data under the Agreement and Section 4.1 below. Customer will disclose or transmit Personal Data to SAS only when the Agreement authorizes Customer to disclose or transmit Personal Data to SAS. For any disclosure or transmission of Personal Data authorized under this Section, Customer will disclose only the Personal Data necessary for the performance of the Services; and will use a mutually-agreed transmission method for transmission of electronic data.

4. SAS Obligations as Processor.

- 4.1. Customer Instructions. SAS will Process Personal Data on behalf of Customer and in accordance with Customer's documented instructions set forth in the Agreement and this Addendum and any other written and mutually agreed instructions provided by Customer to SAS, or as otherwise required by applicable law. SAS will inform Customer without undue delay if, in SAS' opinion, any instruction infringes Applicable Data Protection Laws. SAS shall be entitled to suspend the Processing until either the parties mutually agree to amend the Agreement or this Addendum to modify the instruction or Customer confirms its lawfulness to SAS' reasonable satisfaction. SAS is not, however, obligated to perform a comprehensive legal examination of any instruction from Customer.
- 4.2. Prohibited Activities. SAS shall Process Personal Data only for limited and specified purposes as set forth in the Agreement and this Addendum, and shall not otherwise:
 - 4.2.1 "sell" or "share" Personal Data, as those terms are defined in Applicable Data Protection Laws;
 - 4.2.2 retain, use, or disclose Personal Data outside of the direct business relationship between SAS and Customer; or
 - 4.2.3 except as permitted by Applicable Data Protection Laws, combine Personal Data that SAS receives from or on behalf of Customer with personal information that SAS receives from, or on behalf of, another person or persons, or collects from its own interaction with a Data Subject.
- 4.3. Compliance with Applicable Data Protection Laws. SAS will comply with Applicable Data Protection Laws and will provide a level of privacy protection for Personal Data consistent with the requirements of Applicable Data Protection Laws. SAS will promptly notify Customer if it makes a determination that it can no longer meet its obligations under this Addendum or comply with Applicable Data Protection Laws. Customer shall have the right, upon notice, including from SAS pursuant to the preceding sentence, to take reasonable and appropriate steps to stop and remediate any unauthorized Processing of Personal Data.
- 4.4. Technical and Organizational Security Measures. For any Processing of Personal Data using SAS' hardware, systems or facilities, SAS will implement the applicable technical and organizational security measures that are designed to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access ("**Security Measures**") as set forth in Schedule 2 (Technical and Organizational Security Measures) to this Addendum. Customer has assessed the Security Measures and agrees that the Security Measures provide an appropriate level of security for the Personal Data, taking into account the risks presented by the Processing. SAS may, from time to time, modify the Security Measures, provided, however, that the Security Measures as modified will not reduce the level of protection provided for Personal Data. Customer is solely responsible for providing appropriate technical and organizational security measures for Processing of Personal Data on Customer's hardware, systems or facilities or any hardware, third party systems or facilities made available by Customer.
- 4.5. SAS Personnel. SAS will take appropriate measures to ensure that its employees engaged in the Processing of Personal Data comply with the Security Measures, are bound by confidentiality obligations with respect to all Personal Data Processed hereunder, and process Personal Data only in accordance with this Addendum.
- 4.6. Security Breach. In the event that SAS becomes aware of a Security Breach, SAS will notify Customer of such Security Breach without undue delay and where reasonably practicable not later than 72 hours after having become aware, taking into account the nature of the Processing and the information available to SAS. SAS will take reasonable measures designed to identify the root cause(s) of the Security Breach, mitigate any possible adverse effects and prevent a recurrence. As information regarding the Security Breach is collected or otherwise reasonably becomes available to SAS and to the extent permitted by applicable law, SAS will provide Customer with (i) a description of the nature and reasonably anticipated consequences of the Security Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; (iii) where

possible, the categories and approximate numbers of Personal Data and Data Subjects that were the subject of the Security Breach; and (iv) other information concerning the Security Breach reasonably known or available to SAS that Customer may be required to disclose to a supervisory authority or affected Data Subjects. Customer, however, shall remain solely responsible for fulfilling any Data Subject or supervisory authority notification obligations that are applicable to Controllers under Applicable Data Protection Laws.

- 4.7. Data Subject Requests. Upon Customer's detailed written request, and taking into account the nature of the Processing, SAS will reasonably assist Customer through appropriate technical and organizational measures to fulfill Customer's obligation to respond to Data Subject Requests arising under Applicable Data Protection Laws. SAS will respond to any requests it receives under this Section within a reasonable time, to permit Customer to meet its regulatory guidelines where sufficient notice has been provided to SAS and such timeline is practicable. SAS will forward to Customer any Data Subject Requests that it receives directly from an individual Data Subject, but SAS is not required to respond directly to such Data Subject Requests.
- 4.8. Data Protection Impact Assessments; Prior Consultations. Taking into account the nature of the Processing and the information available to it, SAS will reasonably assist Customer in complying with any data protection impact assessment or prior consultation obligations Customer has under Applicable Data Protection Laws.

5. International Data Transfers.

- 5.1. Customer Authorization for International Transfers. Subject to the terms of this Addendum, Customer authorizes SAS to transfer Personal Data as reasonably necessary for the performance of the Services to any country in which SAS, SAS Affiliates, or Subprocessors maintain facilities.
- 5.2. EEA Restricted Transfers. If and to the extent SAS' performance of the Services involve an EEA Restricted Transfer, the terms of this Section 5.2 will apply with respect to such EEA Restricted Transfer provided that no Alternative Transfer Solution, as defined in Section 5.4, applies.
 - 5.2.1 When SAS is not located in a Third Country and acts as a data exporter with respect to an EEA Restricted Transfer, SAS will enter into the EU Standard Contractual Clauses under Module 3 (Transfer Processor to Processor) with any Subprocessors located in Third Countries that act as data importers and will conduct such EEA Restricted Transfer in accordance with those EU Standard Contractual Clauses.
 - 5.2.2 When SAS is located in a Third Country and acts as the data importer with respect to an EEA Restricted Transfer, SAS hereby enters into the EU Standard Contractual Clauses, which are incorporated by reference herein, with Customer, and with any Related Entities that are permitted to receive or use the Services performed by SAS under the Agreement, each to the extent they act as data exporters in an EEA Restricted Transfer. For the purpose of any such EEA Restricted Transfer, the EU Standard Contractual Clauses will be completed as follows:
 - (a) Module Two (Transfer Controller to Processor) will apply when Customer or the Related Entity is a Controller.
 - (b) Module Three (Transfer Processor to Processor) will apply when Customer or the Related Entity is a Processor.
 - (c) For the purpose of Section II, Clause 8.1 (Modules Two and Three), the Agreement and this Addendum constitute the final and complete instructions to SAS for the Processing of Personal Data as of the date of this Addendum. Any additional or alternate instructions must be mutually agreed upon separately in writing and signed by both parties.
 - (d) For the purpose of Section II, Clause 8.9 (Modules Two and Three), the parties agree that any audits or inspections be conducted in accordance with the "Information and Audits" Section of this Addendum.
 - (e) For the purpose of Section II, Clause 9 (Modules Two and Three), the parties select Option 2 and agree that SAS may engage Subprocessors in accordance with the

“Subprocessing” section of this Addendum.

- (f) For the purpose of Section II, Clause 11 (Modules Two and Three), the parties agree that the optional language in Clause 11(a) will not apply.
- (g) For the purpose of Section II, Clause 13(a) (Modules Two and Three):
 - i. When Customer is established in an EEA Member State, the supervisory authority with responsibility for ensuring compliance by Customer with GDPR as regards to the data transfer shall act as competent supervisory authority.
 - ii. When Customer is not established in an EEA Member State, but falls within the territorial scope of application of GDPR in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1) of GDPR, the supervisory authority of the Member State in which the representative sits within the meaning of Article 27(1) of GDPR is established shall act as competent supervisory authority.
 - iii. When Customer is not established in an EU Member State, but falls within the territorial scope of application of GDPR in accordance with Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of GDPR, the supervisory authority of one of the EEA Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
- (h) For the purpose of Section IV, Clause 17 (Modules Two and Three), the parties select Option 2, and if the data exporter’s Member State does not allow for third-party beneficiary rights, then the law of Ireland shall apply.
- (i) For the purpose of Section IV, Clause 18 (Modules Two and Three), the parties agree that disputes arising from the EU Standard Contractual Clauses shall be resolved by the courts of Ireland.
- (j) Annex I is deemed to be completed with the details set out in Schedule 1 to this Addendum.
- (k) Annex II (Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data) is deemed to be completed with the Technical and Organizational Security Measures set out in Schedule 2 to this Addendum.
- (l) If and to the extent an EEA Restricted Transfer involves Personal Data originating from Switzerland and is subject to the Swiss Federal Act on Data Protection of 19 June 1992 (the “**FADP**”), the EU Standard Contractual Clauses are deemed to be supplemented with an additional annex that provides as follows:
 - i. for purposes of Clause 13 and Annex I.C, the competent Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner;
 - ii. the term “member state” as used in the EU Standard Contractual Clauses must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18.c;
 - iii. references in the EU Standard Contractual Clauses to the GDPR should be understood as references to the FADP; and
 - iv. until entry into force of the revised FADP of 25 September 2020, the EU Standard Contractual Clauses also protect the data of legal entities.

5.3. UK Restricted Transfers. If and to the extent SAS’ performance of the Services involve a UK Restricted Transfer, the terms of this Section 5.3 will apply with respect to such UK Restricted Transfer provided that no Alternative Transfer Solution, as defined in Section 5.4, applies.

- 5.3.1 When SAS is not located in a Third Country and acts as a data exporter with respect to a UK Restricted Transfer, SAS will enter into the EU Standard Contractual Clauses under Module 3 (Transfer Processor to Processor) and the UK Addendum with any Subprocessors located in Third Countries that act as data importers and will conduct such UK Restricted Transfer in accordance with those EU Standard Contractual Clauses and the UK Addendum.
- 5.3.2 When SAS is located in a Third Country and acts as the data importer with respect to a UK Restricted Transfer, SAS hereby enters into the EU Standard Contractual Clauses pursuant to Section 5.2.2 of this Addendum, and the UK Addendum, which are incorporated by reference herein, with Customer, and with any Related Entities that are permitted to receive or use the Services performed by SAS under the Agreement, each to the extent they act as data exporters in a UK Restricted Transfer. For the purpose of any such UK Restricted Transfer:
- (a) Table 1 of the UK Addendum is deemed to be completed with the parties' details and contact information as set forth in Schedule 1 to this Addendum.
 - (b) For the purposes of Table 2 of the UK Addendum, the Addendum EU SCCs are the EU Standard Contractual Clauses entered into between Customer and SAS under Section 5.2.2 of this Addendum.
 - (c) For the purposes of Table 3 of the UK Addendum, the Appendix Information is set forth in Schedule 1 and Schedule 2 to this Addendum.
 - (d) For the purposes of Table 4 of the UK Addendum, the parties select both the Importer and the Exporter, and agree that either of them may end the UK Addendum in accordance with Section 19 thereof.
- 5.4. Alternative Transfer Solutions. If SAS adopts a solution other than the EU Standard Contractual Clauses and/or the UK Addendum that enables the lawful transfer of Personal Data in connection with an EEA Restricted Transfer or UK Restricted Transfer in accordance with GDPR and other Applicable Data Protection Laws, such as binding corporate rules or another approved international data transfer framework (such solution, an "**Alternative Transfer Solution**"), then SAS shall notify Customer in writing and the Alternative Transfer Solution shall apply in lieu of the EU Standard Contractual Clauses and/or the UK Addendum, as applicable, to any EEA Restricted Transfers or UK Restricted Transfers, as applicable, that take place following such written notification.
- 5.5. Supplementary Measures. When and to the extent Personal Data transferred under this Section 5 is subject to GDPR, the following terms will also apply to such Personal Data, in addition to any applicable terms set forth in the EU Standard Contractual Clauses, the UK Addendum, and elsewhere in this Addendum. These terms supplement, but do not vary or otherwise modify, the terms in the EU Standard Contractual Clauses and the UK Addendum.
- 5.5.1 If SAS receives a valid and binding order from any third party for compelled disclosure of Personal Data processed under this Addendum, SAS shall: (a) use reasonable efforts to redirect the third party to request data directly from Customer, (b) promptly notify Customer, unless prohibited by law, and, if prohibited from notifying Customer, use reasonable and lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and (c) use reasonable and lawful efforts to challenge the order for disclosure if and to the extent it is inappropriate or overbroad, including where it conflicts with the law of the European Union or any European Union member state. If, after the steps described in (a) through (c), SAS remains compelled to disclose personal data, SAS will disclose only the minimum amount of Personal Data necessary to satisfy the order for compelled disclosure. For purposes of this Section 5.5.1, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.
- 5.5.2 Nothing in this Addendum restricts Customer's Data Subjects from exercising their rights under GDPR, including their rights to seek compensation from SAS for material or non-

material damage for SAS' breach of this Addendum under, and in accordance with, Article 82 of GDPR.

- 5.5.3 SAS agrees and warrants that it has no reason to believe that the legislation applicable to SAS or its Subprocessors, including in any country to which Personal Data is transferred either by itself or through a Subprocessor, prevents it from fulfilling the instructions received from Customer and its obligations under this Addendum, the EU Standard Contractual Clauses, or the UK Addendum, and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Addendum, the EU Standard Contractual Clauses, or the UK Addendum, it will promptly notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of Personal Data to SAS.

6. Subprocessing.

- 6.1. Authorization to Engage Subprocessors. In connection with SAS' performance of the Services, Customer hereby generally authorizes SAS to appoint as Subprocessors (a) SAS Affiliates and (b) any third-party contractors of SAS or SAS Affiliates, unless otherwise provided in the Agreement. SAS shall make available to Customer a current list of its Subprocessors. SAS will ensure that Subprocessors only Process Personal Data in accordance with this Addendum, and that they are bound by written obligations that require them to provide at least the equivalent level of data protection required by this Addendum. SAS remains responsible for its Subprocessors' compliance with the terms of the Agreement and this Addendum.
- 6.2. Addition or Replacement of Subprocessors. If during the Term SAS intends to add new third party Subprocessors, SAS will notify Customer. Customer may object to a new Subprocessor by providing written notice to SAS no later than thirty (30) days after receiving SAS' notification. SAS will use reasonable efforts either to resolve Customer's objection or to modify its provision of the Services to avoid Processing of Personal Data by the proposed Subprocessor. If Customer's objection cannot be resolved, and SAS cannot reasonably modify its provision of the Services to avoid Processing of Personal Data by the proposed Subprocessor, SAS may suspend or terminate the applicable Agreement or other contractual obligation for the Services, without prejudice to any rights of SAS under the Agreement. Notwithstanding the foregoing, Customer consents to any SAS Affiliate acting as a Subprocessor under this Addendum without the need for further notice.

7. Legally Required Disclosures.

Except where prohibited by law, SAS will use reasonable efforts to notify Customer of any subpoena, judicial process, law enforcement request, or other legally binding order of an executive or administrative agency or other governmental authority (collectively, "**Demand**") that SAS, SAS Affiliates or Subprocessors receive and that relates to Personal Data, in order to permit Customer to seek protection against disclosure. SAS has no responsibility to interact with any governmental authority or other entity making a Demand provided, however, that SAS may disclose Personal Data to such authority or entity in response to a Demand where in SAS' sole discretion such disclosure is necessary to protect SAS' rights or to comply with applicable law.

8. Information and Audits.

- 8.1. Compliance Information. Upon Customer's reasonable request, SAS will provide information to Customer that is sufficient to demonstrate SAS' compliance with its obligations under this Addendum. Customer agrees that any information SAS provides under this Section is confidential and must be subject to mutually-agreeable confidentiality terms prior to disclosure.
- 8.2. Audits and Inspections. If the Agreement permits Customer to conduct a Security Audit, Customer may audit SAS' compliance with the requirements of this Addendum under the same terms, and subject to the same limitations and restrictions, as are set forth in the Agreement concerning Security Audits. If the Agreement does not provide for a Security Audit, Customer may audit SAS' compliance with this Addendum subject to the following terms and conditions:
- 8.2.1 Upon Customer's reasonable written request, SAS will make available to Customer a copy of audit reports related to the Services prepared by a qualified third-party auditor. The audit reports are SAS' Confidential Information under the Agreement. If Customer requires

additional information not contained in the audit reports to comply with its obligations under Applicable Data Protection Laws or a supervisory authority's request, Customer will inform SAS in writing to enable SAS to provide such additional information. Except as otherwise provided in Section 8.2.2 below, Customer agrees to accept the findings in the audit reports, and any additional information provided by SAS, in lieu of requesting an on-site audit.

- 8.2.2 In the event that Customer reasonably demonstrates that information provided by SAS under Section 8.2.1 is not sufficient to satisfy an audit obligation mandated by Applicable Data Protection Laws or a supervisory authority's request, Customer may conduct, at Customer's expense, an on-site audit to verify that SAS is in compliance with its data protection obligations under this Addendum ("**On-Site Security Audit**"). The audit may be conducted by Customer or by an independent third-party auditor mutually acceptable to both parties ("**Auditor**"). Customer will conduct such On-Site Security Audit at the SAS offices where the Services are conducted and during SAS' normal business hours. SAS will not be required during such Security Audit to disclose any information relating to other customers or to third parties. Customer must provide SAS with at least thirty (30) days' written notice prior to conducting an On-Site Security Audit, except that Customer may conduct an On-Site Security Audit with a shorter notice period in the event that (i) Customer is subject to a regulatory authority audit or order with respect to the processing of Personal Data that requires a shorter notice period; or (ii) SAS has notified Customer of a Security Breach. On-Site Security Audits must not interfere with SAS' normal business operations and will not exceed three (3) SAS business days. The Auditor must sign a confidentiality agreement with SAS prior to conducting the On-Site Security Audit and will comply at all times with SAS' security rules, policies and procedures. SAS will cooperate with the Auditor by: (x) making applicable records available; (y) providing copies of such records as requested for review by the Auditor on SAS' premises; and (z) directing SAS employees to reasonably cooperate. Except as set forth in this Section 8.2.2, in no event shall Customer or the Auditor be entitled to access the facilities of, or to otherwise observe any security safeguards maintained by, SAS or its Subprocessors in conjunction with an On-Site Security Audit.

9. Deletion of Personal Data.

After expiration of the Term, SAS will return or otherwise make available, or delete or otherwise render inaccessible, the Personal Data in its possession, unless (i) prohibited by applicable law, or (ii) Customer notifies SAS prior to SAS' receipt of such Personal Data that the Personal Data is subject to laws or regulations requiring specific deletion practices or retention periods and such requirements are specified in the applicable Agreement. The terms of this Addendum will continue to apply to Personal Data until it is returned, deleted, or rendered inaccessible.

10. Enforcement; Limitation of Liability.

Unless Applicable Data Protection Laws require a Related Entity to exercise or seek any remedy under this Addendum directly by itself, Customer shall: (a) exercise any such right or seek any such remedy on behalf of the Related Entity; and (b) exercise any such rights or seek any such remedies in a combined manner for all Related Entities together, rather than separately for each Related Entity individually. The limitations of liability and any exclusions of damages set forth in the Agreement govern the aggregate liability of SAS for all claims arising out of or related to this Addendum, any Schedules or Exhibits thereto, and the Agreement. These limitations of liability and exclusions of damages apply to all such claims, whether arising under contract, tort or any other theory of liability, and any reference to the liability of SAS means the aggregate liability of SAS and all SAS Affiliates together for claims by Customer and all Related Entities. This section is not intended to modify or limit the parties' joint and several liability for Data Subject claims under GDPR Article 82 or the right of contribution under GDPR Article 82. Further, this section is not intended to limit either party's responsibility to pay penalties imposed on that party by a regulatory authority for that party's violation of Applicable Data Protection Laws.

11. Integration; Interpretation; Modifications.

11.1. This Addendum, together with the Agreement, are the parties' complete and exclusive statement

relating to their subject matter. Additional or conflicting terms on current or future Customer or third-party purchasing documents are expressly objected to and rejected. For clarity, this Addendum does not apply to non-binding proposals, memoranda of understanding or letters of intent, regardless of what title is used to describe such documents.

- 11.2. In the event of a conflict between the Agreement, this Addendum, and the EU Standard Contractual Clauses, the order of precedence is: (a) to the extent they apply, the EU Standard Contractual Clauses or UK Addendum; (b) this Addendum; (c) the Agreement.
- 11.3. SAS may make changes to this Addendum from time to time (a) when such changes are required to comply with Applicable Data Protection Laws, or (b) when the changes: (i) are commercially reasonable; (ii) do not result in a material reduction in the level of security provided by SAS for Personal Data; (iii) do not expand the scope of, or remove any restrictions on, SAS' Processing of Personal Data as set forth in Section 4 (SAS Obligations as Processor) of this Addendum; and (iv) do not otherwise have a material adverse impact on Customer's or any Related Entity's rights under this Addendum. When SAS makes changes to the Addendum under this Section 11.3, SAS will post the updated version of the Addendum to <https://www.sas.com/dpa>.

LGL5777/Revised: June2022

SCHEDULE 1

DETAILS OF THE PROCESSING

A. List of Parties

Data Exporter(s):

Name: Customer and/or its Related Entities that are permitted to receive or use the Services performed by SAS under the Agreement between SAS and Customer.

Contact Details: The email and mailing address(es) for Customer's primary contact person(s) as set out in the Order Form.

Activities relevant to the data transferred: Use of Software, Consulting Services, a SAS Cloud offering, or any other offering made available by SAS to Customer pursuant to the Agreement.

Signature and Date: By entering into the Agreement, Customer is deemed to have signed the EU Standard Contractual Clauses entered into by Customer and SAS pursuant to Section 5.2.2 of the Addendum, including their Annexes, as of the effective date of the Agreement.

Role: Controller or Processor, as set forth in Section 2.1 (Roles of the Parties) of the Addendum.

Data Importer:

Name: The SAS entity that is party to the Agreement.

Contact Details: SAS Institute Inc.
SAS Campus Drive
Cary, NC 27513
ATTN: Legal Division / Privacy Officer
privacy@sas.com

Activities relevant to the data transferred: Provision of Software, Consulting Services, a SAS Cloud offering, or any other offering made available by SAS to Customer pursuant to the Agreement.

Signature and Date: By entering into the Agreement, SAS is deemed to have signed the EU Standard Contractual Clauses entered into by Customer and SAS pursuant to Section 5.2.2 of the Addendum, including their Annexes, as of the effective date of the Agreement.

Role: Processor

B. Description of Transfer

Categories of data subjects whose personal data is transferred

The Categories of Data Subjects may include the following:

- Employees and contact persons of:
 - Customer or a Related Entity
 - Customer's or a Related Entity's prospects and customers
 - Customer's or a Related Entity's vendors and suppliers
 - Customer's or a Related Entity's business partners
- Prospects, Customers, vendors, suppliers, and business partners of Customer or a Related Entity (who are natural persons).
- Such other Data Subjects as may be the subjects of Personal Data included in Customer Materials that Customer makes available to SAS for Processing on Customer's behalf in connection with SAS' performance of the Services, as determined and controlled by Customer and set forth in the

SCHEDULE 1

Agreement and any data classification forms completed by Customer pursuant to the Agreement.

Categories of personal data transferred

The Personal Data may include the following categories of data :

- Business contact details
- Personal contact details
- Human Resources Data
- System Access / Usage / Authorization Data
- Contract and Invoice Data
- Such other categories of Personal Data included in Customer Materials that Customer makes available to SAS for Processing on Customer's behalf in connection with SAS' performance of the Services, as determined and controlled by Customer and set forth in the Agreement and any data classification forms completed by Customer pursuant to the Agreement.

The Personal Data will not contain any of the following unless otherwise agreed in the applicable Agreement or data classification forms completed by Customer pursuant to the Agreement:

- (a) government-issued personal identification numbers (including but not limited to social security numbers, driver's license numbers, and passport numbers);
- (b) credit or debit card numbers, personal identification numbers (PIN), passwords or other electronic identification numbers or other information a person uses for payment or to access personal or financial information;
- (c) patient, medical or other protected health information that is subject to the U.S. Health Insurance Portability and Accountability Act of 1996 or any similar national or state laws, rules or regulations;
- (d) any Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or criminal record or history, or that concerns an individual's health or sex life; or
- (e) any classified data or technical data controlled by the International Traffic in Arms Regulations.

Nature and Purposes of Processing

SAS will Process Personal Data as necessary to perform the Services under the Agreement, including for the purposes of: (a) setting up, operating, monitoring, and providing the Services; (b) communicating with Users; and (d) executing other agreed-upon written instructions of Customer.

Period for which Personal Data Will be Retained

Personal Data will be retained for the duration of the Agreement and subject to Section 9 (Deletion of Personal Data) of the Addendum.

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

Transfers will be made on a continuous basis.

For transfers to Subprocessors, the subject matter, nature, and duration of the processing

The subject matter, nature, and duration of processing undertaken by Subprocessors will be the same as set forth in the Addendum and this Schedule 1 with respect to SAS.

C. Competent Supervisory Authority

SCHEDULE 1

Under the Standard Contractual Clauses entered by the parties pursuant to Section 5.2.2 of the Addendum, under Module Two (Transfer Controller to Processor) and Module Three (Transfer Processor to Processor), the supervisory authority will be the competent supervisory authority that has supervision over Customer or the Related Entity, or representative, as applicable, or where Section 5.2.2(g)(iii) applies, the Data Protection Commission of Ireland, in accordance with Section 5.2.2.(g) of the Addendum and Clause 13 of the Standard Contractual Clauses.

SCHEDULE 2

Technical and Organizational Security Measures

For any Processing of Personal Data using SAS' hardware, systems, or facilities, SAS will implement and maintain the technical and organizational security measures described in this Schedule. Customer is solely responsible for providing appropriate technical and organizational security measures for Processing of Personal Data on Customer's systems or facilities or any third-party systems or facilities operated on behalf of Customer.

A. Technical and Organizational Security Measures for all SAS Environments

Security Practices:

- SAS utilizes daily threat assessment and current event feeds to stay up-to-date on security trends and vulnerabilities.
- SAS utilizes endpoint detection & response (EDR) software and host-based firewalls on all client systems.
- SAS utilizes endpoint detection & response (EDR) software on all Windows server systems.
- SAS patches client system operating systems and critical third-party software components monthly.
- SAS patches server systems on a varied schedule based on application and environments.
- SAS implements web-filtering and content enforcement mechanisms for all outbound web requests from its systems.
- All SAS-issued laptops utilize full disk encryption.
- SAS performs web application penetration testing for new and significantly changed Internet-facing web assets.
- SAS conducts global network penetration testing annually.
- SAS performs weekly vulnerability scans for Internet-facing assets.
- All network data transfers must follow SAS-supported encryption protocols.

Network Security:

- All SAS Internet connectivity points utilize firewalls at both ingress and egress points.
- SAS office locations with Internet-facing resources utilize network-based intrusion detection systems and intrusion prevention systems (IDS/IPS).
- SAS practices default-deny for inbound network traffic and strictly controls inbound access via appropriate change control processes.

SCHEDULE 2

- SAS accomplishes logging and address translation at the firewall.
- SAS monitors network configuration changes daily.
- SAS provides protection from unauthorized network access, including by:
 - Recording and auditing server events involving elevated user access and elevated privileges.
 - Reviewing elevated access and authentication logs the next business day.

Email security:

- Email ingress and egress are encrypted via opportunistic transport layer security (TLS).
- Email is scanned for malicious attachments and malicious URLs.
- URLs within email messages are protected with time-of-click reputation assessment.
- Attachments are detonated in a sandbox environment prior to delivery.
- Supplementary phishing and social engineering protections are in place for all inbound messages.
- Abusive mailbox submissions are monitored by SAS Security Operations staff.

Elevated Logical Access:

- Elevated logical access requests require multiple approvals.
- System administrator access is limited and conducted through a secure connection.
- Elevated logical access is promptly removed from users whose employment with SAS is terminated, or who change positions such that access is no longer required to perform their job duties.

Physical Security Controls:

SAS utilizes various physical access controls to protect its systems and data. Those controls vary depending on the location and criticality of data processed, but may include:

- A requirement that security badges be worn and visible at all times.
- Badge readers and/or PIN codes that control access to secure environments.
- Cameras that monitor ingress to and egress data centers, with logging and maintenance of all video recordings.
- A requirement that all external visitors, including non-preferred third-party vendors, register and sign a log sheet upon entering and exiting SAS facilities.

SCHEDULE 2

- Maintenance of an access transaction report that lists all access attempts, successful or unsuccessful, within SAS' data center environments and backup tape vault.
- Uninterruptable Power Supply (UPS) and diesel generators that provide back-up power.
- Fire suppression systems to monitor and prevent fire impact.
- Environmental systems to monitor and alert changes to humidity and temperature.
- Use of multiple Internet providers/gateways to provide internet connection redundancy.

Personnel Security Controls:

- All SAS employees are bound by SAS' security, access, and acceptable use policies.
- All SAS employees complete annual security awareness training.
- SAS removes access and either retains or disables all company assets during the employee termination process.

Security Incident Response:

- SAS' Security Incident and Response Team (SIRT) Process provides a consistent framework for responding to security incidents and providing proper notice as required by law.
- SAS' Product Security Incident and Response Team (PSIRT) process provides a consistent framework for responding to SAS product-related security issues.

Data Destruction Requirements:

- When storage media has reached the end of its useful life, SAS utilizes decommissioning procedures designed to prevent data from being recoverable or exposed to unauthorized individuals.
- SAS uses data safeguarding and sanitization techniques, which may involve encryption, deletion, clearing, overwriting, wiping, purging, degaussing, or destruction, as applicable to the technology.

Security Testing:

SAS maintains procedures to regularly test the effectiveness of its security controls. These procedures include annual global network penetration tests and weekly vulnerability scans for Internet-facing assets.

B. Additional Technical and Organizational Security Measures Applicable to Hosted Environments

This section describes the additional security measures that SAS has implemented for Hosted Environments. For purposes of this Schedule 2, "Hosted Environments" include SAS Software

SCHEDULE 2

environments hosted and/or managed by SAS that are located at SAS' corporate headquarters and co-located data centers, and virtual private clouds at SAS' third party cloud service providers.

Certifications:

- ISO 27001 certification for Hosted environments.
- SSAE 18 Service Organization Control (SOC 2 and 3) Type II certification (achieved for SAS environments that are hosted and/or managed by SAS at SAS corporate headquarters, SAS' co-located data centers, and SAS' virtual private cloud at Amazon Web Services).
 - Above statement is not applicable for Customer Intelligence 360 products.

Network and Logical Security:

SAS maintains controls to monitor and protect its network and production systems against external intrusion. These controls include:

- Secure gateways into and out of SAS' network, implemented through the following measures:
 - Hosted Environment configurations deny services until successful authentication.
 - Access to Hosted Environments from external networks is restricted to secure access connections.
 - Access to Hosted Environments from SAS internal networks is secure and changes to firewall services must be approved.
 - SAS logs all instances of access denial to Hosted Environments.
- All network data transfers to and from Hosted Environments are accomplished using publicly available encrypted protocols as supported by SAS.
- Web applications within Hosted Environments are only accessible via authorized IP addresses unless otherwise specified in the relevant Order Form. SaaS products including Customer Intelligence 360 may not include these allow-list restrictions.
- For externally facing assets in Hosted Environments, integrity and non-repudiation are maintained via digital certificates issued by a trusted certificate authority.
- A Security Information and Event Management system ("SIEM") or a Log Management System that includes infrastructure logs has been implemented for all Hosted Environments.
- Routers for Hosted Environments are configured to allow only necessary protocols to be routed to specific hosts.
- IT systems for Hosted Environments are monitored 24 hours a day, 7 days a week.

SCHEDULE 2

- Hosted Environments are protected from unauthorized access through measures that include:
 - Access control lists that control network devices;
 - Server configurations that record details about accesses; and
 - Privileged access and authentication logs that are regularly monitored, and regular review of all alerts and tickets. For Customer Intelligence 360, an access review is conducted quarterly.
- System patches and security updates are regularly reviewed, approved, and installed as required.
- Privileged logical access is controlled and requires multiple approvals, and SAS conducts quarterly privileged access reviews.
- System administrator access is limited and conducted through a secure connection using multi factor authentication.

Physical Security:

SAS maintains controls that are designed to ensure that access to the hardware at its facilities or Infrastructure as a Service (IaaS) providers that is used to provide the Services is limited to properly authorized individuals (such controls include including badge-readers and multi-factor authentication), and that environmental controls are established to detect, prevent, and control damage to that hardware due to environmental extremes.

Personnel Security:

SAS maintains controls that are designed to ensure that access to Personal Data is limited to personnel who require access to perform the Services. These controls include the following:

- Access to a hosting instance is available only after successful entry of a unique combination of User ID and password.
- Access to the hosted solutions is restricted to those Users who require access to perform their job duties.
- All Users must login with a User ID and password and require encrypted protocols over public networks.

Data Security:

SAS maintains controls that are designed to ensure the security, confidentiality, and integrity of Personal Data that is transmitted to SAS for Processing in connection with the Services. These controls include the following:

- Non-public Customer Materials must be sent to SAS via encrypted protocols except where specifically agreed otherwise in writing by the parties.
- Customer Materials are logically separated within the hosting environment.

SCHEDULE 2

- Backups are securely maintained and use storage that is encrypted at rest.
- Access to Customer Materials is limited according to the principle of least privilege.
- System administrator authorization and server authentication are employed as measures to protect data transfers.
- SAS maintains a vendor management program to evaluate ongoing third-party vendor and supplier performance and the security posture of the vendors and suppliers. The program includes:
 - Periodic audits of suppliers' security configurations to ensure they meet agreed-upon information security obligations. Such audits include all aspects of the security configurations for cloud provider services used to provide the service.
 - Ongoing assessment and periodic requalification of suppliers of critical services to ensure supplier viability during the contract life cycle, as appropriate.

Security Testing:

SAS maintains procedures to regularly test the effectiveness of its security controls, including Penetration testing for new and significantly-changed production applications that are exposed to the Internet.

Business Associate Agreement (SAS as Business Associate)

If Customer is a Covered Entity or a Business Associate and includes Protected Health Information in Customer Materials, execution of an Order Form (“**Agreement**”) will incorporate the terms of this Business Associate Agreement (“**BAA**”) into that Agreement with respect to disclosure of Protected Health Information. Except where this BAA conflicts with the Agreement, all other terms and conditions of the Agreement remain unchanged.

1. Definitions

Except as otherwise defined in this BAA, capitalized terms shall have the definitions set forth in HIPAA, and if not defined by HIPAA, such terms shall have the definitions set forth in the Agreement.

- 1.1. “Breach Notification Rule”** means the Breach Notification for Unsecured Protected Health Information Final Rule.
- 1.2. “Business Associate”** shall have the same meaning as the term “business associate” in 45 CFR § 160.103 of HIPAA.
- 1.3. “Covered Entity”** shall have the same meaning as the term “covered entity” in 45 CFR § 160.103 of HIPAA.
- 1.4. “HIPAA”** collectively means the administrative simplification provision of the Health Insurance Portability and Accountability Act enacted by the United States Congress, and its implementing regulations, including the Privacy Rule, the Breach Notification Rule, and the Security Rule, as amended from time to time, including by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act and by the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule
- 1.5. “PHI”** shall mean “Protected Health Information” as defined in 45 C.F.R. §160.103, limited to the Protected Health Information transmitted, maintained, created or received by SAS from or on behalf of Covered Entity pursuant to the performance of SAS’ obligations under the Agreement.
- 1.6. “Privacy Rule”** shall mean the federal privacy regulations issued pursuant to HIPAA, as amended from time to time, codified at 45 C.F.R. Parts 160 and 164 (Subparts A & E).
- 1.7. “Security Rule”** shall mean the federal security regulations issued pursuant to HIPAA, as amended from time to time, codified at 45 C.F.R. Parts 160 and 164 (Subparts A & C).

2. Permitted Uses and Disclosures

- 2.1. Performance of Agreement.** Except as otherwise limited in this BAA, SAS may use or disclose PHI in connection with the performance of its obligations for, or on behalf of, Covered Entity as permitted or required by the Agreement.
- 2.2. Proper Management and Administration.** Except as otherwise limited in this BAA, SAS may disclose PHI for the proper management and administration of SAS, provided that disclosures are (a) Required By Law, or (b) SAS obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies SAS of any instances of which it is aware in which the confidentiality of the information has been breached.
- 2.3. Data Aggregation Services.** Except as otherwise limited in this BAA, SAS may use PHI to provide Data Aggregation Services to Covered Entity as permitted by 45 C.F.R. §164.504(e)(2)(i)(B) if provided for in the Agreement or as requested by Covered Entity.

- 2.4. **Reporting Violations.** SAS may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. §164.502(j)(1).

3. Responsibilities of SAS

To the extent SAS is acting as a Business Associate, SAS agrees to the following:

- 3.1. **Limitation on Use and Disclosure.** SAS will use and/or disclose PHI only as necessary to provide the Services as permitted or required by this BAA and/or the Agreement and in compliance with each applicable requirement of 45 C.F.R. §164.504(e), or as otherwise Required by Law. SAS will not use PHI for any advertising, Marketing or other commercial purpose of SAS or any third party. SAS shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request.
- 3.2. **Safeguards.** SAS will comply with the Security Rule and use appropriate administrative, physical, and technical safeguards to (a) prevent use or disclosure of PHI other than as provided for by this BAA, and (b) reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that SAS creates, receives, maintains, or transmits on behalf of Covered Entity.
- 3.3. **Reporting.** SAS shall report to Covered Entity: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which SAS becomes aware; (2) any Security Incident of which it becomes aware, provided that notice is hereby deemed given for Unsuccessful Security Incidents and no further notice of such Unsuccessful Security Incidents shall be given; and/or (3) any Breach of Covered Entity's Unsecured Protected Health Information that SAS may discover (in accordance with 45 CFR § 164.410 of the Breach Notification Rule). Notification of a Breach will be made without unreasonable delay, but in no event more than five (5) business days after SAS' determination of a Breach. The notification shall include, to the extent possible, the identification of all individuals whose Unsecured PHI was or is believed to have been involved; a brief description of what happened, including relevant dates; a description of the types of Unsecured PHI involved in the Breach; efforts taken by SAS to investigate and mitigate the effects of the Breach and protect against future Breaches; relevant contact information, and other information reasonably requested by Covered Entity to assist it in fulfilling the requirements of HIPAA. Taking into account the level of risk reasonably likely to be presented by the Use, Disclosure, Security Incident, or Breach, the timing of other reporting will be made consistent with SAS' and Covered Entity's legal obligations.

For purposes of this Section, "**Unsuccessful Security Incidents**" mean, without limitation, pings and other broadcast attacks on SAS' firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of Protected Health Information. Notification(s) under this Section, if any, will be delivered to contacts identified by Covered Entity pursuant to Section 6.7, including through e-mail. SAS' obligation to report under this Section is not and will not be construed as an acknowledgement by SAS of any fault or liability with respect to any Use, Disclosure, Security Incident, or Breach.

- 3.4. **Subcontractors.** In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, SAS will ensure that any agent or subcontractor that creates, receives, maintains or transmits PHI on behalf of SAS agrees to the same requirements, restrictions and conditions that apply to SAS with respect to such information. In addition, SAS shall ensure that any agent or subcontractor to whom it provides ePHI agrees to comply with the Security Rule. SAS shall enter into a written agreement with each such agent or subcontractor, and the terms of such agreement shall incorporate the applicable requirements of, and otherwise comply with, HIPAA.
- 3.5. **Access.** To the extent that SAS maintains PHI in a Designated Record Set on behalf of Covered Entity, provide access, within fifteen (15) days after receiving a written request from Covered

Entity, to such PHI in a Designated Record Set, to Covered Entity, in accordance with the requirements of and as necessary to satisfy the requirements of 45 C.F.R. §164.524.

- 3.6. Amendment.** To the extent that SAS maintains PHI in a Designated Record Set on behalf of Covered Entity, make any amendment(s) to such PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. §164.526 at the request of Covered Entity.
- 3.7. Disclosure to the Secretary.** SAS will make its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by SAS on behalf of, Covered Entity available to the Secretary, at reasonable times during normal business hours, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule, subject to attorney-client and other applicable legal privileges.
- 3.8. Accounting of Disclosures.** SAS will document and make available to Covered Entity within fifteen (15) days after receiving a written request from Covered Entity an accounting of disclosures of PHI about an Individual, in accordance with and as necessary to satisfy the requirements under 45 C.F.R. §164.528
- 3.9. Mitigate.** SAS will mitigate, to the extent practicable, any harmful effect that is known to SAS of a use or disclosure of PHI by SAS or its agents or subcontractors in violation of the requirements of this BAA or HIPAA
- 3.10. Performance of Covered Entity's Obligations.** To the extent SAS has agreed in writing to carry out one or more of a Covered Entity's obligation(s) under the Privacy Rule, comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligation(s).
- 3.11. Additional Notice from Covered Entity.** if notified by Covered Entity of (i) any limitations in Covered Entity notice of privacy practices, (ii) any changes in or revocation of an Individual's permission to use or disclose his/her Protected Health Information, and/or (iii) any restriction on the use or disclosure of Protected Health Information to which Covered Entity has agreed or is required to agree, to comply with any such limitations or restrictions as applicable and necessary in carrying out its duties under the Agreement or this BAA.
- 3.12. De-Identification of PHI.** SAS will use PHI to create de-identified information in accordance with the HIPAA Rules only at the request and direction of Covered Entity. SAS shall not otherwise be permitted to de-identify PHI.

4. Responsibilities of Covered Entity

In addition to any other obligations set forth in the Agreement, including in this BAA:

- 4.1. Covered Entity Notifications.** Covered Entity shall notify SAS of any (a) limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. §164.520, to the extent that such limitation may affect SAS' use or disclosure of PHI, (b) changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect SAS' use or disclosure of PHI, and (c) restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. §164.522, to the extent that such restriction may affect SAS' use or disclosure of PHI.
- 4.2. Minimum PHI Necessary.** Covered Entity shall provide, or direct its other business associates to provide, to SAS only the minimum PHI necessary to accomplish the Services.
- 4.3. Consent or Authorization.** Covered Entity shall obtain any consent or authorization that may be required by any applicable laws or regulations prior to furnishing, or directing any of its other business associates to furnish, any PHI to SAS.
- 4.4. No Impermissible Requests.** Covered Entity shall not request SAS to Use or Disclose Protected Health Information in any manner that would not be permissible under HIPAA if done by a Covered Entity (unless permitted by HIPAA for a Business Associate).

- 4.5. Transmission of ePHI.** Covered Entity shall not transmit any ePHI to SAS by any electronic media or means, including via email and/or over the Internet, unless the Agreement expressly authorizes such transmission. SAS shall not be liable to Covered Entity for any damages arising out of Covered Entity's transmission of ePHI to SAS in violation of this Section, anything in the Agreement or this BAA notwithstanding.
- 4.6. Safeguards and Appropriate Use of Protected Health Information.** Customer is responsible for implementing appropriate privacy and security safeguards to protect its Protected Health Information in compliance with HIPAA. Without limitation, it is Customer's obligation to:
- (a) Not include Protected Health Information in: (1) information Customer submits to technical support personnel through a technical support request or to community support forums; and (2) Customer's address book or directory information.
 - (b) Implement privacy and security safeguards in the systems, applications, and software Customer controls and configures.

5. Term and Termination

- 5.1. Term.** The Term of this BAA shall be effective as of the Effective Date, and shall terminate upon the final expiration or termination of the Agreement unless earlier terminated in accordance with Section 5.2 of this BAA.
- 5.2. Termination for Cause.** When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, SAS shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.
- 5.3. Effect of Termination.** Except as provided in paragraph (b) of this Section 5.3, upon termination of this BAA, for any reason, SAS shall return or destroy all PHI received from Covered Entity, or created, received, or maintained by SAS on behalf of Covered Entity, and shall retain no copies of such PHI. In the event that SAS determines that returning or destroying the PHI is infeasible, SAS shall provide to Covered Entity written notification of the conditions that make return or destruction infeasible, and shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as SAS maintains such PHI.

6. Miscellaneous

- 6.1. Incorporation; Entire Agreement.** The BAA, together with the Agreement as amended by this BAA, constitutes the entire agreement between the parties with respect to the subject matter contained herein.
- 6.2. Amendment.** This BAA may be amended or modified only in a writing signed by the parties. The parties agree to take such action as is necessary to amend this BAA from time to time as is necessary to make it conform to the requirements of HIPAA.
- 6.3. Survival.** The respective rights and obligations of SAS under Sections 3.3, 5.3 and 6.10 of this BAA shall survive the termination of this BAA.
- 6.4. Interpretation.** All PHI shall be subject to and treated in accordance with this BAA and shall not otherwise be considered "Confidential Information" as defined in the Agreement. Any ambiguity in this BAA shall be resolved to permit compliance with HIPAA and shall be construed in light of any applicable interpretation or guidance on the HIPAA Rules issued by HHS or the Office of Civil Rights from time to time. In the event of any inconsistency between the BAA and the Agreement, the terms and conditions of this BAA shall control. In the event of an inconsistency between the provisions of this BAA and mandatory provisions of HIPAA, the

provisions of HIPAA shall control. Where provisions of this BAA differ from those mandated by HIPAA, but are nonetheless permitted by HIPAA, the provisions of this BAA shall control.

- 6.5. No Third Party Beneficiaries or Assignment.** Nothing express or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever. No party may assign or delegate its respective rights or obligations under this BAA without the prior written consent of the other party.
- 6.6. Independent Contractors.** None of the provisions of this BAA are intended to create, nor will they be deemed to create any relationship between the parties other than that of independent contractors.
- 6.7. Written Notice.** Except as otherwise stated herein, written notice shall be deemed to have been duly served if delivered in accordance with the terms of the Agreement.
- 6.8. Waiver.** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.
- 6.9. Certain Provisions Not Effective in Certain Circumstances.** The provisions of this BAA relating to the HIPAA Security Rule shall not apply to SAS if SAS does not receive, create, maintain, or transmit any ePHI from or on behalf of Covered Entity. If SAS' access to ePHI shall be from Covered Entity's information systems and environment and no ePHI is removed or copied from such systems or environment by SAS or otherwise placed on SAS' information systems or environment, then the HIPAA Security Rule shall not apply to SAS' information systems or environment.
- 6.10. Additional Rights and Limitations.** In the event of a Breach that is caused by SAS' failure to implement and maintain the safeguards required by the Security Rule, as direct damages under the Agreement, SAS will be liable to Covered Entity for actual reasonable and necessary costs and expenses that Covered Entity incurs in providing legally-required notice to any Individuals or third parties pursuant to 45 C.F.R. §§164.404 and 164.406, subject to the limitations set forth the Agreement, provided that: (a) SAS shall not be liable for any damages associated with any Breach that is attributable in whole or in part to an act or omission of Covered Entity or any third party engaged by Covered Entity; (b) SAS shall only be liable for damages associated with a Breach for which an act of SAS or its subcontractor is the sole and proximate cause; (c) SAS' liability for actual reasonable and necessary costs and expenses as set forth in this Section shall be limited to those costs and expenses Covered Entity incurs within one (1) year of the date Covered Entity becomes aware of the Breach; and (d) the foregoing is SAS' sole and exclusive monetary obligation to Covered Entity with respect to the Breach. Some jurisdictions do not allow limitations of liability or exclusions for damages associated with data security breaches, so certain provisions of this Section may not apply; however, they apply to the greatest extent permitted by applicable law.

Carahsoft Technology Corporation (“Reseller”) is authorized to resell the SAS Institute Inc. (“SAS”) Offerings pursuant to the agreement to which these terms are attached. The Universal Terms and associated addenda apply to any SAS Offering that Customer orders from Reseller under Reseller’s contract with Customer. SAS will act as a subcontractor to Reseller. The Universal Terms take precedence over any conflicting terms in Customer’s Order Form.

SAS Universal Terms

These Universal Terms apply to all Offerings. To order an Offering, Customer will submit a Purchase Order to Reseller that incorporates these Universal Terms and other Offering-specific addenda. [Definitions](#)

1. Permitted Use

1.1 **Usage Rights.** This section describes the standard usage or access rights for Offerings. The Order Form may contain additional or different usage or access rights.

1.1.1 For any SAS Cloud Offering, Customer may access the System during the Term.

1.1.2 For any Software Offering installed outside of a System, SAS grants Customer a license to use the Software during the Term.

1.1.3 If the Offering includes Work Product, SAS grants Customer a royalty-free license to use the Work Product. If the Work Product relates to Software or a System, Customer will use the Work Product only in connection with the applicable Software or System and during the Term of the Agreement for the Software or System.

1.2 **Benefit.** Customer will use the Offering solely for the benefit of its operations in the Territory. If the Territory is global or includes more than one country, then Customer's Related Entities may also benefit from use of or access to the Offering.

1.3 **Restrictions.**

1.3.1 All license grants and usage rights are nonexclusive, nonassignable and nontransferable.

1.3.2 Customer will not use any Offering or Documentation to: (a) bring an intellectual property infringement claim against SAS; or (b) create or assist a third party in creating an offering that competes with SAS.

1.3.3 Customer may use any Documentation only to support Customer's use of the related Software.

1.3.4 Customer will not use any Offering in a time-sharing or service provider arrangement.

1.4 **Users.** This Permitted Use section extends to Users.

2. Agreement Term

2.1 **Effective Date; Term.** The Agreement is effective upon acceptance of the Order Form and will remain in effect for the Term.

2.2 **Termination.** When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, SAS shall proceed diligently with performance of this Agreement, pending final resolution of any request

for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. Obligations in the Agreement that by their nature are continuing survive expiration or termination. In addition, the terms of the Agreement will continue to apply if SAS continues to provide an Offering to Customer while the parties are in good faith negotiations to renew the Offering. SAS' provision of the Offering during any such negotiation is not fee waived.

If the Agreement terminates or expires, Customer will stop using the Offering and delete any media, Product Authorization Codes, or Documentation provided by SAS. Customer may terminate the Agreement as set forth in www.sas.com/termination. A current version of this policy is attached hereto.

3. Fees

3.1 **Fees.** Fees are listed in the Order Form in accordance with the GSA Schedule Pricelist.

3.2 **Payment.** Payments are due net thirty (30) days. SAS may designate an affiliate or a third party to invoice and/or collect payment on its behalf.

3.3 **Upgrades.** Customer must contact SAS to change any factor impacting the Pricing Metric or applicable usage or access rights. These changes may result in additional Fees calculated and invoiced based on the date of the change.

3.4 **Taxes.** Customer is exempt from all federal, state and local taxation, except real estate taxes, under 12 U.S.C. §531. Accordingly, SAS shall not charge the Customer any federal, state or local taxes.

3.5 **Third Party Payments.** Customer may designate a third party to receive invoices and make payments on Customer's behalf. Customer will be responsible for any related charges assessed by the third party. Payment of all Fees remains Customer's ultimate responsibility.

4. Technical Support

4.1 **General.** Technical support for the Software or System is included during the Term as documented in SAS' technical support policies, at <https://support.sas.com/en/technical-support/services-policies.html>, which may be updated from time to time. Customer may obtain additional support services from SAS by executing an Order Form and paying additional Fees to SAS.

Technical support also includes access to all new releases, updates, bug-fixes, security patches and

other corrective code that SAS makes generally available. Customer agrees to use reasonable efforts to install such content for Software not hosted by SAS. If Customer chooses not to install the current release of the Software or instructs SAS not to install the current release of the Software in a System, the level of technical support will diminish over time. During ongoing development, SAS may rename Offerings or add, change or delete individual components or functionality in new releases of the Software or System. .

4.2 Customer Contacts and Notification.

Customer must establish knowledgeable technical contacts who are qualified to provide SAS with information necessary for SAS to diagnose and remedy any problems. When requesting technical support, Customer will notify SAS of any modifications to the Software or System not made by SAS. Failure to comply with these terms may result in longer response and resolution times.

5. Intellectual Property

The Agreement does not transfer any ownership rights. SAS and its licensors retain title to the Offering, any Documentation, source code, and any techniques, skills, concepts or know-how SAS utilizes or develops while performing the Agreement. Customer retains ownership to Customer Materials and any data Customer derives from using an Offering. The Software source code is a SAS trade secret. Customer and Users will not access source code or attempt to reverse engineer, reverse assemble or decompile the Software or System. Customer and Users will not remove any copyright or proprietary rights notice from any Offering. The Agreement does not limit any rights Customer may have under any open-source license covering any open-source component included in the Offering.

Use of any online training provided with an Offering but not separately listed on the Order Form is governed by the terms of the Agreement.

6. Customer Materials

6.1 **Usage Rights.** Customer grants SAS a nonexclusive, nonassignable, nontransferable and royalty-free license to use the Customer Materials solely to perform the Agreement.

6.2 **Data Classification Forms.** Before providing any Customer Materials to SAS, Customer will complete any data classification forms that SAS requests. Customer will only transmit Customer Materials to SAS using SAS-approved methods.

6.3 **Format and Protection.** Customer's failure to provide any required Customer Materials in a mutually agreed upon format and timeframe, and in

a usable condition, may delay SAS' performance of the Agreement. The parties will manage any resulting schedule changes through a change control process, and additional Fees may apply.

Customer is responsible for: (a) the integrity of the Customer Materials; (b) backing up the Customer Materials, and (c) mitigating the risks inherent in storing or transmitting the Customer Materials via the System, including the risk of data loss.

6.4 **Exclusions.** SAS' warranties, indemnities and technical support set forth in the Agreement do not apply to Customer Materials.

6.5 Customer Materials Used in a System.

6.5.1 Customer must obtain SAS' prior written approval before using Customer Materials owned by a third-party data provider in the System. If any third-party data provider requires that SAS sign a separate data use agreement in order to use such data to perform the Agreement, then Customer, SAS and the provider will sign a three-party agreement. Notwithstanding the terms of any such data use agreement, the data provided by the third party will be deemed Customer Materials, and the Customer warranties and indemnification applicable to Customer Materials in the Agreement will apply.

6.5.2 If SAS believes the Customer Materials violate applicable law or third-party rights, SAS may either: (a) require Customer to remove the Customer Materials from the System; or (b) disable the Customer Materials.

6.5.3 Customer is responsible for: (a) providing or arranging for the provision of all support, maintenance, and upgrades for Customer Materials, including up-to-date virus protections; and (b) coordinating the timing of such activities with SAS. Customer may direct the Customer Materials provider to contact SAS on Customer's behalf for technical support issues if the provider believes the issue is connected to the System.

6.5.4 SAS may disable or remove Customer Materials in the event of any emergency situation or any threat or perceived threat to the System related to the Customer Materials. SAS will not be responsible for any adverse performance impact to the System or Downtime attributable to Customer Materials or to any such disengagement. In addition, SAS is not responsible for any compromises to the confidentiality, integrity, or availability of the System or Customer Materials that are attributable in whole or in part to Customer's use of Customer Materials.

7. Preproduction Offerings

7.1 **Preproduction Offerings.** During the Term, SAS may give Customer the opportunity to preview Preproduction Offerings at no cost to Customer so that Customer may provide feedback to SAS. No

additional Order Form is required for Customer to preview a Preproduction Offering, regardless of whether the Preproduction Offering is a version of a production Offering that Customer has ordered via an Order Form or separate technology. Customer will not use Preproduction Offerings for production purposes.

7.2 No Warranty. SAS PROVIDES PREPRODUCTION OFFERINGS “AS IS.” SAS’ warranties and indemnification obligations set forth in the Agreement do not apply to Preproduction Offerings. SAS does not guarantee that any Preproduction Offering or functionality will be made generally available.

7.3 Disclaimers. NEITHER CUSTOMER, SAS, NOR SAS’ THIRD-PARTY LICENSORS ARE LIABLE FOR DIRECT, SPECIAL, INCIDENTAL, INDIRECT, CONSEQUENTIAL, PUNITIVE, OR RELIANCE DAMAGES (ARISING IN TORT, CONTRACT OR OTHERWISE) RELATED TO THE PREPRODUCTION OFFERING, EVEN IF THEY HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. SAS AND SAS’ THIRD-PARTY LICENSORS ARE NOT LIABLE FOR ANY THIRD-PARTY CLAIMS AGAINST CUSTOMER RELATED TO A PREPRODUCTION OFFERING. THE PARTIES MAKE THESE EXCLUSIONS IN CONSIDERATION OF THE LICENSES GRANTED UNDER THE AGREEMENT.

7.4 Hosted Preproduction Offering. If SAS makes the Preproduction Offering available via a hosted environment, Customer will comply with the terms of use that SAS specifies in writing.

8. SAS Warranties and Disclaimers

8.1 Intellectual Property Warranty. SAS warrants it has the right to license the Software or Work Product or provide the Offering to Customer. Customer’s exclusive remedy for SAS’ breach of this warranty is set forth in the *Indemnification by SAS* section.

8.2 Virus Warranty; Conformance with Documentation Warranty. SAS warrants that when delivered, each commercially available release of the Software will not contain a virus and will substantially conform to its Documentation. As Customer’s exclusive remedy for breach of this warranty, SAS, at its option, will: (a) repair the Software; (b) replace the Software; or (c) terminate the applicable Order Form and refund the Fees paid for the Software during the then-current annual period or any prepaid Fees under the Order Form.

8.3 Skilled Personnel Warranty. SAS warrants that the Consulting Services will be performed by skilled personnel. As Customer’s exclusive remedy for breach of this warranty, SAS will refund the Fees paid for the Consulting Services at issue.

8.4 WARRANTY DISCLAIMERS. SAS AND ITS THIRD-PARTY LICENSORS DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ARISING AS A RESULT OF CUSTOM OR USAGE IN THE TRADE OR BY COURSE OF DEALING. SAS MAKES NO WARRANTY THAT THE SOFTWARE OR THE SYSTEM WILL OPERATE ERROR-FREE OR WITHOUT INTERRUPTION OR THAT ANY DATA TRANSMISSIONS TO, FROM, OR THROUGH THE SYSTEM WILL BE COMPLETELY SECURE. SAS DOES NOT WARRANT OR REPRESENT THAT CUSTOMER’S USE OF THE OFFERING ALONE WILL RESULT IN CUSTOMER’S COMPLIANCE WITH ANY APPLICABLE LAW.

9. Customer Warranties

9.1 Intellectual Property Warranty. Customer warrants that: (a) it has the right to provide the Customer Materials to SAS; and (b) Customer and Users will comply with any third-party usage rights and applicable laws related to the Customer Materials. The exclusive remedy for breach of these warranties is set forth in the *Indemnification by Customer* section.

9.2 Compliance Warranty. Customer warrants that the publication, transmission and receipt of all Customer Materials complies with all applicable laws including, without limitation, laws relating to trademarks, copyrights, defamation, consumer protection, personal privacy and false or deceptive trade practices.

10. Exclusions of Damages; Limitation of Liability

10.1 Exclusion of Damages. Neither Customer, SAS, nor SAS’ third-party licensors are liable for special, incidental, indirect, consequential, punitive, or reliance damages (arising in contract, tort or otherwise) even if they have been informed of the possibility of such damages. Neither SAS nor SAS’ third-party licensors are liable for any third-party claim against Customer. SAS’ third-party licensors are not liable for any direct damages. The foregoing limitation of liability shall not apply to (1) personal injury or death resulting from Licensor’s negligence; (2) for fraud; or (3) for any other matter for which liability cannot be excluded by law.

10.2 Limitation of Liability. THE TOTAL AMOUNT CUSTOMER MAY RECOVER FROM SAS FOR ALL CLAIMS ARISING FROM OR RELATING TO THE AGREEMENT IS LIMITED IN THE AGGREGATE TO THE FEES CUSTOMER HAS PAID FOR THE OFFERING AT ISSUE

DURING THE APPLICABLE ANNUAL PERIOD IN WHICH THE CLAIM AROSE.

10.3 Applicability. This section does not apply to the *Indemnification by SAS* section, the *Indemnification by Customer* section, or to either party's violation of the other's intellectual property rights. The limitations in this section will apply even if any of the remedies provided in the *SAS Warranties and Disclaimers* section fail of their essential purpose. Some jurisdictions do not allow limitations of liability or exclusions of certain types of damages so certain provisions of this section may not apply to Customer. However, the provisions apply to the greatest extent permitted by applicable law.

11. Indemnification by SAS

Provided Customer complies with the Agreement, SAS will have the right to intervene to defend and indemnify Customer for any third-party claim against Customer for: (a) any copyright, patent, trade secret or other intellectual property rights violation relating to the Software, Work Product, or any Software or Work Product included in a SAS Cloud Offering; or (b) bodily injury, death or damage to tangible property, arising solely from actions for which SAS is legally responsible. Tangible property does not include software or data. Customer will promptly notify SAS in writing of any such claim. Customer will allow SAS to control the litigation or settlement of any such claim and will cooperate with SAS in the investigation, defense and settlement. SAS will indemnify Customer by paying for the costs and attorneys' fees Customer incurs at SAS' direction and any judgment finally awarded against Customer or settlement approved by SAS. Customer may participate at Customer's own expense. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

If any intellectual property claim is made or, in SAS' opinion, is likely to be made, SAS may: (i) modify the Software or Work Product; (ii) obtain rights for Customer to continue using the Software or Work Product; or (iii) terminate Customer's license to use the Software or Work Product and refund any Fees paid by Customer for the then-current annual period or for the Work Product at issue. Customer will abide by SAS' decision.

SAS' indemnification obligation does not apply to claims based on: (1) Customer's combination of the Software or Work Product with other software or materials; (2) Customer's modification to the Software or Work Product; (3) prior versions of the Software if Customer had not installed the latest version or updates to the Software prior to the date the claim arose as instructed by SAS; or (4)

Customer's unique specifications for the Work Product.

12. Reserved

13. Confidential Information

Each party acknowledges that it may have access to certain Confidential Information. The recipient will use the discloser's Confidential Information only to perform its obligations under the Agreement. SAS may also use Customer's Confidential Information to provide Customer sample analysis for other SAS Offerings or Preproduction Offerings. Recipient will not disclose discloser's Confidential Information received in connection with the Agreement to any third parties without Discloser's prior written approval. This restriction does not apply to information that is: (a) generally available to the public; (b) released by discloser without restriction; (c) independently developed or acquired by recipient; (d) known to the recipient prior to receipt from discloser; or (e) revealed pursuant to court order or as required by applicable law, provided that recipient uses reasonable efforts to promptly notify discloser of such requirement prior to compliance in order to permit discloser to seek protection against disclosure. SAS may also: (a) report the terms of the Agreement to SAS' third-party licensors and partners solely as required by agreements between SAS and its third-party licensors and partners; and (b) list Customer as a SAS customer in SAS' annual report or other materials. Recipient's obligations of confidentiality for each item of discloser's Confidential Information will continue for five (5) years from the date of initial disclosure. However, confidentiality obligations for Personal Data or source code will not expire. For the purpose of this section, SAS' affiliates and subcontractors are not "third parties." Unless specifically authorized in the Order Form, neither party will disclose source code. Confidential Information may be subject to full or partial disclosure under the Freedom of Information Act, 5 U.S.C. 552.

14. Data Protection and Personal Data

Customer will not disclose or transmit Personal Data to SAS unless: (a) specifically authorized under the Order Form; (b) authorized by an Addendum incorporated into the Order Form; or (c) required for technical support. In such event, the SAS Data Processing Addendum available at <https://www.sas.com/dpa> will apply to SAS' processing of Personal Data. A current copy of the SAS Data Processing Addendum is attached hereto. If the Personal Data contains Protected Health Information as defined by and subject to the

US Health Insurance Portability and Accountability Act, the Business Associate Addendum available at [sas.com/baa](https://www.sas.com/baa) is incorporated into the Agreement with respect to such disclosure. A current copy of the Business Associate Addendum is attached hereto.

To the extent applicable, SAS will also comply with the SAS Business Customer Privacy Policy available at https://www.sas.com/en_us/legal/privacy.html, which is subject to change at SAS' reasonable discretion. A current copy of the SAS Business Customer Privacy Policy is attached hereto. Changes will not result in a material reduction to the level of protection provided by SAS for any Personal Data during the Term.

15. Insurance

During the Term, SAS Institute Inc. will keep the following insurance policies in force:

(a) Workers Compensation – Statutory (in the amounts required by applicable law);

(b) Employer's Liability – USD \$1,000,000 per occurrence; bodily injury by accident or disease, including death;

(c) Commercial General Liability – USD \$1,000,000 combined limit per occurrence and USD \$2,000,000 aggregate; bodily injury, personal injury and property damage, including blanket contractual liability; and

(d) Automobile Liability (if vehicles are brought on Customer's premises) – USD \$1,000,000 combined limit per occurrence; bodily injury and property damage covering owned, non-owned and hired vehicles.

Evidence of coverage is available at: https://www.sas.com/en_us/legal/evidence-of-insurance.html.

16. Applicable Law

16.1 The validity, interpretation and enforcement of this Agreement, including Offering terms, will be governed by and construed in accordance with the Federal laws of the United States without giving effect to the conflicts of laws provisions thereof or the United Nations Convention on Contracts for the International Sale of Goods. This Agreement is subject to the Contract Disputes Act of 1978, as amended (41 U.S.C. 601-613). Failure of the parties to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this Agreement shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. In the event the

Uniform Computer Information Transactions Act (UCITA) or any similar federal or state laws or regulations are enacted, it will not apply to this Agreement, and the governing law will remain as if such law or regulation had not been enacted.

16.2 **Export and Import Restrictions.** US export laws and regulations apply to the Offering and any other SAS-provided technology ("**Controlled Material**"). The Controlled Material originates from the United States. Both parties agree to comply with these and other applicable export and import laws and regulations, except as prohibited or penalized by law ("**Trade Law**"). Customer warrants that Customer and its Users are not: (a) prohibited by Trade Law from accessing Controlled Material without US government approval; (b) located in or under control of any country or other territory subject to general export or trade embargo under Trade Law; or (c) engaged in any of the following end-uses: nuclear, chemical or biological weapons; nuclear facilities not under International Atomic Energy Agency safeguards; missiles or unmanned aerial vehicles capable of long-range use or weapons delivery, military training or assistance, military or intelligence end-use in Russia or in any country in Country Group D:5 of the United States Export Administration Regulations; deep water, Arctic offshore or shale oil or gas exploration involving Russia or Russian companies, or Russian energy export pipelines. Customer will not import or use any data within the System that is subject to the US International Traffic in Arms Regulations. United States export classification information for SAS software is available at <http://support.sas.com/adminservices/export.html>.

17. General

17.1 **Subcontracting.** SAS may subcontract its performance under the Agreement. However, such subcontracting arrangement does not relieve SAS of its obligations to Customer under the Agreement.

17.2 **Customer Responsibilities.** Customer will: (a) verify the accuracy of its data input and output while using the Offering; (b) duplicate, document and protect all data and software Customer uses with the Offering; (c) for SAS Cloud Offerings, assume responsibility for any damages resulting from Customer's decision to continue running a prior version of the Software in the System that SAS has informed Customer is no longer eligible for SAS' standard technical support; (d) inform all Users of the relevant terms of the Agreement and be responsible for their adherence to such terms; (e) keep records of where any Software is installed and used; (f) keep records of the extent of usage of the

Software or System relative to the applicable Pricing Metrics and usage rights and provide a copy of such records to SAS upon request; (g) designate a single delivery contact for Product Authorization Codes and installation media and a single billing contact for invoices; and (h) use the Offering consistent with the SAS Responsible Use Policy, available at www.sas.com/responsibleuse.

17.3 Customer Feedback. SAS may use any feedback related to any Offering or Preproduction Offering in any format and any ideas, concepts, know-how, formulas, designs, improvements, inventions, techniques or processes contained in that feedback, whether or not patentable.

17.4 Severability. If a court of competent jurisdiction finds any part of the Agreement unenforceable, that part is excluded, but the remainder remains in full force and effect.

17.5 No Waiver. Failure to require compliance with a part of the Agreement is not a waiver of that part. Nothing in the Agreement waives any remedy SAS may have under the Agreement at law, in equity, or otherwise.

17.6 Non-Assignment. Assignments are subject to FAR Clause 52.232-23, Assignment of Claims (JAN 1986) and FAR 42.12 Novation and Change-of-Name Agreements.

17.7 Audit. Upon thirty (30) business days' notice to Customer, SAS may conduct an audit during Customer's normal business hours to verify Customer's compliance with an Order Form. If the audit reveals that Customer owes additional fees, Customer will pay the amounts owed. Audits shall be conducted no more than once during any annual period.

17.8 Injunctive Relief. Because monetary damages are inadequate to remedy a breach of SAS' or its third-party licensors' intellectual property rights, to the extent permitted by law, SAS may protect those intellectual property rights through temporary restraining orders or injunctions without posting bond.

17.9 Force Majeure. Except as may be otherwise provided herein, this Agreement is subject to FAR 52.212 -4 (f) Excusable delays. (JUN 2010).

17.10 Independent Contractors. SAS, its employees, and subcontractors are acting as independent contractors and not as employees or agents of Customer. Neither party has the authority to bind the other party.

17.11 Third Party Rights; No Lease. Unless specifically stated in the Order Form, the Agreement does not confer any rights upon any third parties. This Agreement does not lease any interest in real property to Customer.

17.12 Reserved

17.13 Updates to Terms. SAS may change the non-material terms and condition of the terms set forth in the URLs listed in the Order Form or incorporated into the Agreement from time to time. However, if the change results in a material degradation of the Customer's rights under the Agreement, SAS will provide Customer with written notice of the change by posting the notice on www.sas.com/contract-with-sas-archive.

17.14 Languages. The parties enter into the Agreement in English. However, Customer or SAS may enter into all or a portion of the Order Form in a non-English language. In that event, the Order Form will be binding as written but any addenda incorporated into the Order Form will be binding in English. SAS may make the Agreement available in other languages for Customer's convenience. However, the English language version controls unless otherwise required by applicable law. SAS may invoice Customer in English.

17.15 Complete Agreement. If SAS provides an Order Form as a click agreement, the Agreement will be binding upon both parties upon Customer's acceptance. The Agreement is the parties' complete statement relating to its subject matter. SAS rejects any additional or conflicting terms on purchase orders or other purchasing documents. Except as set forth in the Updates to Terms section, the Agreement may not be modified by any side agreement or arrangement between SAS and Customer, written or oral, that purports to modify the Agreement and is not accepted in writing by an authorized representative of both parties.

Definitions

These defined terms are used in the Universal Terms, an Addendum and/or an Order Form. SAS may define additional terms in an Order Form or Addendum.

1. **“Addendum”** means any addendum incorporated into an Order Form.
2. **“Agreement”** means the collective set of terms identified in the Order Form. Invoices also form part of the Agreement.
3. **“Application Monitoring Software”** means software specified by SAS and required to collect data to verify the availability and performance of the Software.
4. **“Authorized Environment”** means the physical hardware, virtual machine, private cloud, public cloud account, or other environment where the Software is installed. If a pricing metric refers to “Authorized Hardware,” that term will be interpreted to mean “Authorized Environment.”
5. **“Committed Period”** means a period during which neither party may terminate an Order Form for convenience, except as set forth in the *Termination* section above.
6. **“Confidential Information”** means confidential information of the other party that is either marked as confidential or should be reasonably understood to be considered confidential due to its nature. Confidential Information includes source code, Customer Materials, Personal Data and the Product Authorization Code.
7. **“Connectivity Tool”** means individually assigned credentials which will enable access to Customer’s computing system via Customer’s VPN, Remote Desktop Protocol, or any other remote connection with multi-factor authentication and scoped access to data.
8. **“Consulting Services”** means SAS consulting services identified on an Order Form.
9. **“Customer”** means the customer entity identified on an Order Form.
10. **“Customer Budget”** means the amount of money Customer makes available for payment of Fees for the performance of Time and Materials Consulting Services. Applicable taxes and travel and living expenses are not included in Customer Budget.
11. **“Customer Materials”** means any materials that Customer provides to SAS or directs SAS to obtain.
12. **“Customer’s Infrastructure”** means Customer’s information technology infrastructure, including computers, software, databases, electronic systems (including database management systems) and networks, whether operated by Customer or a third party.
13. **“Deliverable”** means the tangible or intangible items identified in an Order Form that SAS agrees to deliver as part of Fixed Price Consulting Services.
14. **“Documentation”** means the official user documentation that SAS may make available for Software at <https://support.sas.com/en/documentation.html>.
15. **“Fee”** means the fee that Customer will pay to SAS under the Order Form.
16. **“Fixed Price”** means a pre-defined project model where SAS provides Consulting Services for a set Fee.
17. **“Issue Tracking System”** means the system that SAS provides to report, track and monitor issues associated with the Software and/or System.
18. **“License Period”** means the period during which Customer is authorized to use the Software.
19. **“Offering”** means the SAS offering listed on the Order Form, which may include Software, Consulting Services, a SAS Cloud offering, or any other offering made available by SAS.
20. **“Option Period”** means any annual period following the initial term where Customer may agree to renew the Order Form for a renewal Fee specified in the Order Form.
21. **“Order Form”** means the electronic or written ordering document entered into between Reseller and Customer that specifies the Offering, Fee and other commercial terms.
22. **“Personal Data”** means information relating to an identified or identifiable natural person.

23. **“Pre-Installation Requirements Document”** means a document that SAS provides to Customer detailing activities, specifications and other requirements Customer must complete in preparation for installation of Software and provision of the System.
24. **“Preproduction Offering”** means an offering that is not generally available.
25. **“Prerequisite Software”** means any third party software required for use with the Software as defined at <http://support.sas.com/resources/thirdpartysupport/index.html>.
26. **“Pricing Metric”** means the metric used to determine the Fee.
27. **“Product Authorization Code”** means a code that enables the Software to operate for the applicable License Period.
28. **“Related Entity”** means a separate legal entity that is controlled by, is under common control with, or controls Customer. The term "control" means: (a) for commercial entities, ownership of more than fifty percent (50%) of the voting stock or assets of an entity; or (b) for non-profit or governmental entities, statutory or other documented legal authority over the general budget and contracting rights of an entity.
29. **“RMS”** means remote managed services Offering identified on the Order Form.
30. **“SAS”** means SAS Institute Inc. unless another SAS entity is defined in the Order Form.
31. **“SAS Cloud”** means Hosted Managed Services, Subscription Services, XaaS, or other hosted Offerings made available by SAS.
32. **“Sensitive Information”** means (a) credit or debit card numbers, personal identification numbers (PIN), passwords or other similar information used for payment or to access personal or financial information; (b) patient, medical or other protected health information; (c) genetic data, biometric data, or data about an individual’s criminal history; (d) government-issued personal identification numbers (such as social security numbers, driver’s license numbers, or passport numbers); (e) classified or technical data controlled by the US International Traffic in Arms Regulations; or (f) materials that require a United States export license, license exception or other United States government authorization.
33. **“Software”** means SAS software, including its embedded subcomponents, licensed to Customer under an Order Form or accessed by Customer in a System.
34. **“Subscription Period”** means the period during which Customer is authorized to use the SAS Cloud Offering.
35. **“Subscription Service”** means the subscription service Offering identified on the Order Form.
36. **“System”** means any hosted environment provided in connection with a SAS Cloud Offering.
37. **“Term”** means twelve (12) months, or another initial time period if specified in the Order Form, and any subsequent renewal period.
38. **“Territory”** means global, unless otherwise set forth in the Order Form.
39. **“Time and Materials”** means a consultative model where (a) SAS provides Consulting Services at hourly or daily rates; and (b) the only Deliverables are SAS' time and a limited license to any Work Product resulting from the Consulting Services.
40. **“Universal Terms”** means the terms that apply to all Offerings.
41. **“User”** means any individual authorized by Customer to access an Offering.
42. **“Work Product”** means computer code or other materials delivered by SAS in connection with Consulting Services.

Software Addendum

Exhibit A to Universal Terms

This Addendum applies only to Software licenses.

2. Annual Licenses

License Periods are annual unless otherwise set forth in the Order Form.

3. License Renewal

The parties may agree to renew the Software license for additional License Periods. Renewal is accomplished by Reseller executing a written order for the renewal term and sending an invoice for the applicable Fee and Customer paying the invoice.

4. Renewal Fees

The Order Form may specify renewal Fees for a multi-year Term or Option Period(s). If the Order Form does not specify the renewal Fee for the upcoming License Period, Reseller will use reasonable efforts to provide Customer ninety (90) days' advance notice of the renewal Fee.

5. Invoicing

Reseller will invoice Customer for the Fee for the first License Period when Customer submits its Order Form. Reseller will invoice Customer for any renewal Fees annually in advance of each annual License Period.

6. Multi-Year Initial Term

The Order Form may specify a multi-year Term consisting of multiple annual License Periods and will set forth a payment schedule under which the multi-year Fee is paid upfront or on an installment basis. The multi-year Term may consist of a Committed Period and/or Option Periods. Multi-year terms are contingent upon appropriations. Customer will pay the Fee for the Committed Period even if Customer discontinues its use of the Software prior to the expiration of the Committed Period. However, either party may terminate the Agreement for cause according to the *Termination* section of the Universal Terms.

7. Product Authorization Code

When Reseller receives the Fee for each License Period, SAS will provide Customer with a Product Authorization Code valid for that License Period. Customer may need to apply a new Product Authorization Code for changes to the Authorized Environment, operating system or Software version. SAS is not required to provide the Product Authorization Code if Customer is in breach of the Agreement or has not paid any undisputed Fees for the Software.

8. Authorized Environment

The Authorized Environment and any back-up environment must be controlled by Customer or its Related Entities, employees or contractors, including third party cloud providers. Customer will notify SAS of changes to the Authorized Environment. Some Software is not available for use on all types of Authorized Environments.

9. Installations

Except as otherwise set forth in the Order Form, the Software license entitles Customer to one (1) complete instance of the Software in a production environment. Processor cores or license capacity cannot be shared across or used to create multiple production environments. Customer may install the Software on an unlimited number of non-production environments unless the Pricing Metric for the Software is based on the number of installations or the Order Form otherwise limits the number of installations.

10. Pricing Metrics

Unless the Pricing Metric is based on the processing capacity of the Authorized Environment or the number of Users, the Pricing Metric quantity is determined by combining the quantity associated with Customer and Related Entities benefitting from the use of the Software.

If the Pricing Metric is based on the number of Users, the Pricing Metric quantity is determined by combining the quantity of Users authorized by Customer or Related Entities to access the Software.

If the Pricing Metric is based on the processing capacity of the Authorized Environment, the Pricing Metric quantity is calculated separately for each Authorized Environment used for production purposes based on the processing capacity of the Authorized Environment.

If Customer expands the use of the Software to benefit additional Related Entities and such use results in an increase to pricing metric quantities, Customer will notify SAS and pay any applicable additional Fees according to the *Upgrade* section of the Universal Terms.

Users may use the Offering for the benefit of Customer and its Related Entities, subject to the applicable Pricing Metric. Unless the Pricing Metric is based on the processing capacity of the Authorized Environment, the Pricing Metric quantity is determined by combining the quantity associated with Customer and its Related Entities benefitting from the use of the Offering. If Customer expands the use of the Offering to benefit additional Related Entities, Customer will notify SAS of any increase to the Pricing Metric quantity and pay any applicable additional Fees. If the Pricing Metric is based on the processing capacity of the Authorized Environment, the Pricing Metric quantity is calculated separately for each Authorized Environment used for production purposes based on the processing capacity of the Authorized Environment.

Consulting Services Addendum

Exhibit B to Universal Terms

This Addendum applies only to Consulting Services. To purchase Consulting Services, Customer will enter into an Order Form with SAS that incorporates the Universal Terms, this Addendum and any other Offering-specific terms.

1. Consulting Services

SAS will provide the Consulting Services on either a Fixed Price basis or a Time and Materials basis as described in the Order Form. Consulting Services do not include continued support or maintenance of any Work Product, unless such continued support or maintenance is detailed in the Order Form.

2. Time and Materials Consulting Services

This section applies only to Time and Materials Consulting Services.

2.1 **Invoicing.** Reseller will invoice Customer monthly for Fees due.

2.2 **Customer Budget.** If the Order Form sets forth a Customer Budget, SAS will not perform Services or charge Fees exceeding such Customer Budget without an amendment to the Order Form to increase the Customer Budget. Customer is not obligated to spend all of the Customer Budget.

3. Fixed Price Consulting Services

This section applies only to Fixed Price Consulting Services.

3.1 **Invoicing.** Reseller will invoice Customer for the Fees according to the schedule in the Order Form.

3.2 **Acceptance.** Customer will accept or reject a Deliverable within ten (10) business days of delivery. If Customer does not reject a Deliverable within this timeframe, the Deliverable is deemed to have been accepted. Customer must notify SAS in writing to reject a Deliverable and must specify the nature and scope of the deficiencies.

If Customer rejects a Deliverable, the parties will use reasonable efforts to follow these timeframes. Within five (5) business days after receipt of the rejection notice, SAS will either correct the deficiencies or propose the manner and timeframe for correcting the deficiencies. Customer will accept or reject any proposal from SAS for correcting any deficiencies within five (5) business days after receipt of SAS' proposal. Customer will accept or reject the corrected Deliverable within five (5) business days of SAS' delivery.

If Customer rejects SAS' proposal for correcting any deficiencies or rejects the corrected Deliverable, SAS may terminate the Agreement for the Consulting Services and refund the Fees paid for the Deliverable. In such event, Customer will delete or destroy the Deliverable.

If the Order Form does not specify any Deliverables, then the Services are deemed accepted as they are performed.

4. Customer's Responsibilities

Customer will:

- (a) provide accurate information and access to Customer personnel required for SAS to perform the Consulting Services;
- (b) review any Work Product and Deliverables as SAS reasonably requests;
- (c) back up all systems, data or software that SAS will access when performing the Consulting Services;
- (d) implement reasonable measures to prevent SAS' inadvertent access to any Confidential Information not necessary for SAS' performance of the Consulting Services;
- (e) make available facilities and equipment reasonably required for SAS to perform any on-site Consulting Services;
- (f) provide any regulatory requirements to SAS for review in advance of the Consulting Services. Any regulatory requirements that impact the scope of the Consulting Services are subject to the *Change Management* section below; and
- (g) provide and use a Connectivity Tool to limit and control SAS' access to the systems and data required for SAS to perform the Consulting Services. If individually assigned access is unavailable, Customer may permit SAS remote access via screen sharing applications (such as WebEx or Zoom). SAS will use the Connectivity Tool regardless of whether access occurs remotely, at Customer's facility, or using SAS' or Customer's laptops or other hardware.

SAS is not liable for any performance delays caused by Customer's failure or delay to perform these responsibilities.

5. Taxes, Travel and Living Expenses

Fees do not include travel expenses. SAS will invoice Customer monthly for actual travel and living expenses SAS incurs while performing Consulting Services. Customer agrees to pay any travel expenses in accordance with FAR 31.205-46 and the Federal Travel Regulation (FTR) Customer shall only be liable for such travel expenses as approved by Customer and funded under the applicable ordering document. SAS or its authorized reseller as applicable shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k).

6. Change Management

For any change to the scope of Consulting Services or the assumptions set forth in the Order Form, SAS will prepare a written change order describing: (a) the changes; (b) the impact of the changes on the Consulting Services and the project schedule; (c) the estimated timetable; and (d) any additional Fees and cost.

Customer's project manager will respond in writing to a change order within five (5) business days. If the change requires payment of additional Fees, SAS will provide a proposed amendment to the Order Form. Until the parties mutually agree on the change order and sign an amendment, if required, SAS will continue to perform the Consulting Services as if the change order does not apply.

7. Customer Project Manager

Customer will designate one or more project managers to be Customer's primary contact(s) with SAS.

8. Time Limitations

Customer will not bring any claim against SAS related to the Work Product or Consulting Services more than one (1) year after the termination or completion of the Consulting Services under the applicable Order Form.

Pricing Metrics

Exhibit C to Universal Terms

The following pricing metrics apply to the Software if the applicable pricing metrics is referenced in the applicable Order Form.

Authorized Users – The Fee is based on the total number of Authorized Users. “Authorized Users” means the total number of Users, identified by unique User IDs, authorized to access and use the Offering.

Authorized SAS User - The Fee is based on the total number of Authorized SAS Users. “**Authorized SAS User**” means an individual User, identified by a unique User ID, who is authorized by Customer to use the Offering for tasks other than solely viewing or interacting with reports created by Authorized SAS Users (“**Reports**”). There is no limit on the number of individuals authorized to view or interact with Reports.

Decisions - The Fee is based on the total number of Decisions supported by the Software during each annual License Period. “**Decision**” means a query to the Software that results in one or more recommendations for an individual consumer or a process initiated using the Software that results in a batch output that represents one or more individual recommendations. For batch processing or in-database deployments, each record that the Software scores is counted as a single Decision.

Total Tax Revenue in US Dollars (in Billions). The Fee is based on the total tax revenue, expressed in United States dollars, assessed by Customer and processed through the Offering. Any conversion to United States dollars required will be based on the rate of exchange published on the last business day of the month prior to the effective date by OANDA, or other publication as directed by SAS, available at oanda.com.

SAS Tax Compliance – Permitted Scope - Users may use SAS Tax Compliance Software solely to assess and act upon issues related to tax and revenue compliance.

Processed Benefit Value in US Dollars (in Billions) – The Fee is based on the **Processed Benefit Value**, expressed in United States dollars. “Processed Benefit Value” means the total value of the monetary or non-monetary benefits, excluding administrative costs, distributed by Customer to a receiving organization, entity or individual related to a social benefit program or scheme and processed through the Offering. Any conversion to United States dollars required will be based on the rate of exchange published on the last business day of the month prior to the effective date by OANDA, or other publication as directed by SAS, available at www.oanda.com.

SAS Payment Integrity for Social Benefits – Permitted Scope - Users may use SAS Payment Integrity for Social Benefits solely to detect and act upon potential fraudulent or improper activities and cost containment opportunities within government provided or mandated social benefit programs.

SAS Payment Integrity for Health Care – Permitted Scope - Users may use SAS Payment Integrity for Health Care solely to detect and act upon potential fraudulent or improper activities and cost containment opportunities in health care programs.

SAS Financial Crimes Analytics – Permitted Scope – Users may use SAS Financial Crimes Analytics solely to detect, monitor, analyze and investigate financial crimes.

SAS Law Enforcement Intelligence - Permitted Scope - Users may use SAS Law Enforcement Intelligence solely to manage public safety analysis, intelligence and investigations.

SAS Government Management – Permitted Scope - Users may use SAS Government solely to detect and investigate improper or suspicious activities, entities or events related to government operations; provided the Offering cannot be used for detection and investigation activities related to health care fraud, tax and revenue compliance or social benefit programs.

Additional Production Site for Solutions - The Fee is based on the total number of environments that Customer may use for production purposes.

Cores - The Fee is based on the aggregate number of processor cores, or virtual processor cores, on which the Offering is installed or the computation and processing occurs across all Authorized Environments used for production purposes.

SAS Enterprise Miner - Permitted Scope - Users may use components of the SAS Enterprise Miner personal client (including, but not limited to, Base SAS and SAS Enterprise Guide) and the SAS Enterprise Miner thin clients only for exploring and analyzing Customer data provided from the server where the SAS Enterprise Miner server components are licensed and installed.

Total Users - The Fee is based on the total number of Users (not concurrent) who access the Software during the applicable License Period.

Document Pages - The Fee is based on the total number of Document Pages successfully returned by the Optical Character Recognition engine as indicated in the resulting payload file. A

"**Document Page**" is a single image in PNG, JPG or JPEG format or a single page within a multi-page document in PDF or TIFF format.

SAS Payment Integrity for Procurement – Permitted Scope - Users may use SAS Payment Integrity for Procurement.

Processed Expenditures - The Fee is based on total value, expressed in United States dollars, of Customer's Expenditures processed through the offering. "**Expenditure**" means any direct and indirect costs incurred by Customer in its operations. Any conversion to United States dollars required will be based on the rate of exchange published on the last business day of the month prior to the effective date, and each renewal date thereafter, by OANDA Corporation or other publication as directed by SAS, solely to detect and act upon potential fraudulent or improper activities associated with Customer's procurement and other operating expenses.

SAS Viya Workbench – The following terms apply specifically to SAS Viya Workbench

- a) The Subscription Period for SAS Viya Workbench will begin on the date that SAS notifies the Customer that the System is available for access.
- b) Unless the parties otherwise agree, the Order for SAS Viya Workbench will be administered pursuant to a private plan or offer through a mutually agreed upon third-party cloud provider's marketplace ("**Marketplace**"). Upon receipt of Customer's order, SAS or its Reseller will create a private plan or offer reflecting the terms of the order for Customer's acceptance through the Marketplace.
- c) SAS may process information about Customer's configuration and use of the SAS offering ("Usage Data") and Account Data (as defined below) to: (a) manage Customer's accounts; (b) assist SAS with troubleshooting Customer issues, (c) provide and improve SAS offerings; and (d) provide Customer insights, service and feature announcements and other reporting. SAS may also process aggregated and/or anonymized Usage Data (including, for clarity, Usage Data that does not allow a third party to identify Customer as the source of the information) to develop new services and features and promote SAS offerings, including, for example, through analyses of patterns and trends. SAS' processing of Usage Data and Account Data, and any other use of information described in this Section, will at all times be subject to SAS' obligations under the Universal Terms, including Section 13 (Confidentiality) and Section 14 (Data Protection and Personal Data). "Account Data" means information about Customer provided to SAS by Customer or Customer's third party cloud provider in connection with the creation or administration of SAS offerings, such as first and last name, user name and email address of a

User, IP addresses or Customer's contact information. Customer will ensure all Account Data is accurate at all times and will not include Sensitive Information in Account Data.

- d) SAS and its Reseller may share information regarding the Marketplace Order with the third-party cloud provider's marketplace and will process Usage Data and Account Data in connection with the calculation of Fees and associated fees due to the third-party cloud provider.
- e) The Offering includes access to optional or required Non-Hosted Software to utilize the Offering's full functionality. Customer may install any Non-Hosted Software in an Authorized Environment and access the Non-Hosted Software only in conjunction with Customer's authorized usage of the Subscription Service. "Non-Hosted Software" means SAS software included with a SAS Cloud Offering that Customer installs in a physical, virtual, private cloud, or public cloud computing environment that Customer or its contractor controls.
- f) Customer will provide SAS access to Customer's Subscription Services instance(s), as SAS reasonably requests. Access may include administrative access privileges.

Subscription Terms – The following terms apply to any offering identified as a subscription offering, including Viya Workbench

- a) **Subscription Service** - The Subscription Service includes access to a System containing Software and other technology installed in a SAS-managed cloud environment. Customer must procure a separate subscription for each instance of the Subscription Service that Customer accesses.
- b) **Subscription Periods** Subscription Periods are annual unless otherwise noted.
- c) **Invoicing** Reseller will invoice Customer for the Fee for the first Subscription Period when the Subscription Period begins. Reseller will invoice Customer the renewal Fee for any renewal Subscription Period.
- d) **Multi-Period Committed Period** Reseller's quote may specify a multi-period Committed Period consisting of multiple Subscription Periods and will set forth a payment schedule under which the multi-period Fee is paid upfront or on an installment basis. Customer will pay the Fee for the Committed Periods even if Customer discontinues its use of the Offering prior to the expiration of the Committed Periods.
- e) **Access Credentials** SAS may require Users to register for a profile on SAS' website to obtain access to the System.
- f) **Customer Responsibilities** Customer is responsible for: (a) Customer's infrastructure, including communication links and any other technology or hardware required for the System to operate properly between Customer and SAS; (b) the security of access credentials, including ensuring only authorized Users have access to the System or their respective passwords; and (c) any virus Customer introduces into the System through Customer Materials or otherwise. Customer will notify SAS immediately upon becoming aware of any loss or theft of their password or any unauthorized use of the password.
- g) **Personal Data**
 - i) **Personal Data.** Customer may use Personal Data in the System. The *Confidential Information* and *Data Protection and Personal Data* sections of the Universal Terms apply to the Personal Data.
 - ii) **SAS Obligations.** Upon expiration or termination of the contract, SAS will delete or render inaccessible all Personal Data in the System, unless the contract specifies

different retention practices required for compliance with applicable law. SAS may: (a) retain one copy of the Personal Data as necessary to comply with legal, audit or internal SAS requirements; and (b) defer the above activities to the extent and for the duration that SAS cannot reasonably and practically expunge Personal Data from the System. As long as SAS retains any Personal Data in the System, the *Security* section of this Addendum and the *Data Protection and Personal Data* section of the Universal Terms will continue to apply to such Personal Data.

- h) **Sensitive Information.** Unless authorized in the contract, Customer will not use Sensitive Information in the System or transmit Sensitive Information to SAS. If Customer uses or transmits any Sensitive Information in the System in violation of this section, Customer will reimburse SAS for any costs associated with its removal.
- i) **Prohibited Activities** Customer and Users will not use the System to: (a) send spam or other unsolicited marketing or communications; (b) infringe on any party's intellectual property or privacy rights; (c) send or store harassing, abusive, libelous, or obscene materials; (d) falsify or delete transmission information, including headers, return mailing, and Internet protocol addresses; (e) misuse or abuse passwords, confidential information, software, equipment, networks or network devices of SAS or any third party; (f) download the Software, software, or data other than the Customer Materials made available by SAS for Customer's use as permitted under the Agreement via the System; (g) impair the functionality of the System; (h) perform, or cause to be performed, any external penetration or security testing of the System; (i) violate any applicable laws or regulations; or (j) violate the rules of any other service provider engaged by or for the benefit of Customer. Users will not use any open source software in connection with the System if the license to the open source software requires that any part of the System be disclosed or distributed in source code form, made available free of charge, or modifiable without restriction. Customer will promptly notify SAS and use best efforts to remedy any violations of this section by Users. SAS may suspend access to the System if Customer violates this section.
- j) **Security** SAS will employ reasonable security measures designed to: (a) protect the System against unauthorized access, usage, or other threats; and (b) protect Confidential Information, including Personal Data, against unauthorized access, use, alteration, destruction, or disclosure. Such measures are set forth in SAS' Technical and Organizational Security Measures document available at: <https://www.sas.com/TOMS>.

Except as expressly specified in the Agreement, SAS does not represent or guarantee that the System complies with any applicable laws that impose specific data security obligations for the storage or processing of Customer Materials. Customer is solely responsible for determining the suitability of the System in light of any such applicable laws.

- k) **Additional Termination Provisions** SAS may temporarily suspend Customer's System access if Customer fails to cure either of the following conditions: (a) Customer's use of the System or the Customer Materials poses a security risk to the System or any other SAS customer, may harm the System or any other SAS customer, or may subject SAS or any third party to liability; or (b) applicable law prohibits SAS from providing the System to Customer.

SAS may temporarily suspend System access upon five (5) days' written notice in the event Customer uses the System for fraudulent or illegal activities. If a cloud service provider terminates its agreement with SAS to provide their facilities for the System, SAS may, upon at least one hundred twenty (120) days' written notice to Customer, either (a) relocate the System to an alternate internet data center; or (b) if relocation is not commercially reasonable, terminate the agreement and refund to Customer a pro rata portion of any Fees paid by Customer for the time remaining in the Term.

- l) **Microsoft Products** If the System includes any products owned by Microsoft Corporation, the Microsoft terms are available at:

https://www.sas.com/content/dam/SAS/legal/micro_softproductsenglish.pdf.

- m) **Effect of Non-Renewal or Termination** SAS will make portions of the System accessible to Customer at no additional charge for a period of thirty (30) days following the end of the then current Subscription Period for the sole limited purpose of downloading or exporting Customer Materials and other outputs from the use of the Subscription Service. SAS has no obligation to retain Customer Materials or other outputs from the use of the Subscription Service after such 30-day period and thereafter will delete or render inaccessible all Customer Materials and other outputs unless the Contract specifies different retention practices required for compliance with applicable law.
- n) **Disclaimer of Third-Party Actions** SAS exercises no control over the flow of information to or from the System, SAS' network, or other portions of the internet. Such flow depends in large part on the performance of internet services provided or controlled by third parties. At times, actions or inactions of such third parties can impair or disrupt connections to the System. SAS will use commercially reasonable efforts to take all actions it deems appropriate to avoid or remedy such events, but SAS cannot guarantee that such events will not occur. **SAS DISCLAIMS ANY AND ALL LIABILITY RESULTING FROM OR RELATED TO INTERNET OR NETWORK FAILURES. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THE AGREEMENT, SAS DISCLAIMS ANY AND ALL LIABILITY ARISING FROM ACTIONS OR INACTIONS OF A THIRD PARTY.**



Termination for Convenience Policy

This Termination for Convenience Policy (the “**Policy**”) is effective October 1, 2023.

Termination for Convenience Right. A Customer may terminate an Agreement, without cause and without further charge or expense, at any time upon thirty (30) days’ written notice to SAS sent to licensing@sas.com.

This right to terminate under this Policy is subject to Customer and its Related Entities contemporaneously terminating all Agreements in place with SAS. However, if Customer is a partner who has entered into the Agreement for the benefit of an end user, then Customer’s right to terminate under this Policy is subject to Customer contemporaneously terminating all Agreements that Customer has entered into with SAS for the benefit of that end user and end user’s Related Entities. Any fees due from Customer or Related Entities to SAS for the software, SAS Cloud or Excluded Offerings for the period prior to the termination date will become immediately due.

Required Verifications. On or before the expiration of the thirty (30)–day notice period, Customer and its Related Entities must delete all versions of the software and cease accessing the SAS Cloud. Customer must deliver the following verifications to SAS at the address above:

- (a) a statement signed by Customer’s authorized signatory verifying deletion and cessation of access;
- (b) authorization from an authorized signatory of all Related Entities who have entered into an Agreement verifying that Customer has the authority to terminate the Agreement(s) on their behalf; and
- (c) authorization from an authorized signatory of any third party or end user for whom Customer licenses or uses the software or SAS Cloud (such as in a distributor, reseller or service provider arrangement) verifying that such entities have granted Customer the authority to terminate the Agreement(s).

Refund. Within thirty (30) days of SAS’ receipt of all necessary verifications described above, SAS will provide Customer and/or Related Entities with a pro-rata refund of pre-paid software license or SAS Cloud fees related to all terminated Agreements. The refunded fees will be calculated based on the number of days remaining during the pre-paid term (which for purposes of this calculation will begin on the date on which SAS receives all applicable verifications).

Ongoing Obligations. Neither SAS nor Customer will have any obligations under the terminated Agreements except for those obligations identified in the Agreement as surviving its termination or expiration.

This Policy does not apply to Excluded Offerings. If an Agreement contains both: (a) software or SAS Cloud offerings, and (b) Excluded Offerings, then the terms of the Agreement will continue to apply to the Excluded Offerings as set forth in the Agreement.

Termination Upon the End of a Term. This Policy does not modify any other rights Customer has to terminate or not renew software licenses or SAS Cloud offerings under the terms of the Agreement. For example, the Customer may choose not to renew any individual software or SAS Cloud offering at the end of its committed term as set forth in the Agreement without exercising this Policy.

Definitions

Solely for the purpose of interpreting this Policy, the following definitions will control over any conflicting definitions in the Agreement.

“Agreement” means an annual or multi-year software license or SAS Cloud agreement between Customer and SAS.

“Customer” means the entity or partner who has entered into an Agreement with SAS.

“Excluded Offerings” means consulting services, training, enhanced support, or perpetual software licenses or any other offering made available by SAS that is not software or a SAS Cloud.

“Related Entity” unless otherwise defined in the Agreement means a separate legal entity that is controlled by, is under common control with, or controls Customer. However, if Customer is a partner who has entered into an Agreement for the benefit of an end user, then “Related Entity” means a separate legal entity that is controlled by, is under common control with, or controls end user. The term "control" means: (a) for commercial entities, ownership of more than fifty percent (50%) of the voting stock or assets of an entity; or (b) for non-profit or governmental entities, statutory or other documented legal authority over the general budget and contracting rights of an entity.

“SAS” means SAS Institute Inc. and any of its subsidiaries, excluding JMP Statistical Discovery LLC or IDaaS, LLC.

“SAS Cloud” means hosted managed services, subscription services, XaaS, or other hosted offerings made available by SAS.

LGL6040

Last Revised: 01Oct2023