



Snowflake Partner Network (SPN) Program Agreement

Effective Date: June 10, 2025

This Snowflake Partner Network (SPN) Program Agreement (“**Agreement**”) is entered into by and between Snowflake (defined below) and the entity (“**Partner**” or “**you**”) that has accepted this Agreement and will accessing the Partner Portal or participating in the Snowflake Partner Network Program (the “**SPN Program**”). It takes effect on the date set forth above (“**Effective Date**”).

BY INDICATING ACCEPTANCE TO THIS AGREEMENT, ACCESSING THE PARTNER PORTAL, OR PARTICIPATING IN ANY SPN PROGRAM ACTIVITIES (INCLUDING USE OF ANY SPN PROGRAM MATERIALS OR BENEFITS), PARTNER ACCEPTS ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF PARTNER DOES NOT AGREE TO THIS AGREEMENT, NEITHER PARTNER NOR YOU ARE AUTHORIZED TO ACCESS THE PARTNER PORTAL, PARTICIPATE IN SPN PROGRAM ACTIVITIES, OR USE ANY SPN PROGRAM MATERIALS.

IF YOU SIGN UP FOR THE SPN PROGRAM OR PARTNER PORTAL USING AN EMAIL ADDRESS FROM YOUR EMPLOYER OR ANOTHER ENTITY, OR IF YOU ARE AN EMPLOYEE, CONTRACTOR OR AGENT OF AN ENTITY, THEN (A) YOU WILL BE DEEMED TO REPRESENT THAT ENTITY, (B) YOU HEREBY BIND THAT ENTITY TO THIS AGREEMENT AND REPRESENT AND WARRANT THAT YOU HAVE AUTHORITY TO DO SO AND (C) THE WORD “YOU” OR “PARTNER” BELOW WILL REFER TO THAT ENTITY. THE RIGHTS AND BENEFITS GRANTED UNDER THIS AGREEMENT, INCLUDING ANY BENEFITS OF THE SPN PROGRAM, ARE EXPRESSLY CONDITIONED UPON ACCEPTANCE BY SUCH AUTHORIZED PERSONNEL. THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN AGREEMENT SIGNED BY PARTNER.

1. PARTNER PROGRAM.

1.1. Overview. Thank you for registering to participate in Snowflake’s SPN Program. The SPN Program allows partners to take advantage of several partnership benefits based on the partnership tiers and other terms described in the SPN Program’s Guidelines.

1.2. Non-Exclusivity. This Agreement is non-exclusive and does not prohibit either party from entering into any alliance, partner, referral, resale, customer or other agreement with any party at any time provided it otherwise remains in compliance with this Agreement, including its provisions regarding Confidential Information.

1.3. Program Communications. We may use the contact details Partner and Partner Personnel provide to send information about Snowflake, the SPN Program or other information that we think may be of interest to partners. By creating accounts on the Partner Portal, you give us permission to send these communications to you and your Partner Personnel who use the Partner Portal.

1.4. Use of Snowflake Service. For clarity, this Agreement does not grant Partner the right to resell, distribute or otherwise make available Snowflake Technology to anyone, nor does it govern or permit access to or use of the Snowflake Service (including for demo purposes or as part of Partner’s product or service offerings). Partner shall not engage in these activities except as may be agreed to pursuant to a separate agreement with Snowflake.

2. BENEFITS AND ACTIVITIES.

2.1. Access to Partner Portal. Snowflake’s Partner Portal allows Partner to view its SPN Program status, access Training Materials and take advantage of other SPN Program benefits. Subject to the terms and conditions of this Agreement, Snowflake hereby grants Partner a limited, non-exclusive, nontransferable, non-sublicensable right during the Term to access (and to permit Partner Personnel to access) the Partner Portal solely internally in connection with its SPN Program activities. Snowflake’s Privacy Notice (currently available at

<https://www.snowflake.com/privacy-policy/>) applies to the use of the Partner Portal, including to any account information or other Partner Data that Partner or Partner Personnel submit through the portal. Partner must keep its credentials secure and must notify Snowflake immediately of any breach of security or unauthorized use of its account. If any Partner Personnel stops working for Partner, Partner must promptly terminate that person’s access to its Partner Portal account.

2.2. Training Materials. Snowflake’s SPN Training Materials are designed to help Partner Personnel learn about the Snowflake Service and related offerings. Subject to the terms and conditions of this Agreement, Snowflake hereby grants Partner a limited, non-exclusive, nontransferable, non-sublicensable right during the Term to access and use the SPN Training Materials solely for internal training of Partner Personnel. For clarity, Partner may also receive Snowflake training classes ordered from Snowflake via a Snowflake order form or online ordering portal. Such training classes and associated Training Class Materials are subject to the governing agreement specified on such order form and the Training SOW. Except as otherwise expressly stated in the Training SOW, Training Class Materials received as part of a training class may only be used internally by the specific Partner Personnel who attended the class.

2.3. Referral Program. Where specified in the Guidelines, Partner may participate in Snowflake’s optional referral program during the Term. The referral program (including any referral commissions) is subject to this Agreement and the Referral Program Terms located in the Partner Portal (including any eligibility requirements in the Referral Program Terms). If you do not wish to participate in the Referral Program, you may opt-out as specified in the Referral Program Terms.

2.4. Other Program Benefits. Participation in other SPN Program tiers, benefits and activities is optional. These tiers, benefits and activities are described in the Snowflake Partner Network Program Guide and in applicable Guidelines and are also subject to those descriptions and terms. Where indicated, these activities may require invitation and acceptance by Snowflake, which may be granted or denied in its sole discretion. Partner acknowledges and agrees that eligibility for any SPN Program benefits and activities is conditioned upon its continued

compliance with this Agreement and the requirements and terms in the applicable Guidelines. In connection with the SPN Program, the parties may also discuss participation in other, mutually acceptable joint sales activities, such as submission of proposals to prospective clients and/or responding to requests for information from a prospective client. Participation in such additional joint sales activities is at each parties' discretion.

2.5. Use Restrictions. Without limiting the other restrictions in this Agreement, Partner must not (and must not assist others to): (a) copy, transfer, distribute, sublicense, or otherwise provide access to the Partner Portal or SPN Training Materials to a third party (except Partner Personnel working on Partner's behalf); (b) modify, translate, or excerpt content from the Partner Portal or Training Materials; (c) use the Partner Portal or Training Materials to develop any derivative works (including further internal or external training coursework or materials) or any products, services or programs competitive with Snowflake's; (d) use the Partner Portal or Training Materials for any third-party's benefit or in connection with activities not related to the SPN Program; or (e) use, transfer, distribute, sublicense or otherwise provide access to any Training Class Materials by anyone other than Partner Personnel who attended the applicable class, except as otherwise expressly permitted by the Training SOW. The licenses granted herein do not permit any of the foregoing uses. Partner agrees not to register, nor attempt to register, in any jurisdiction any Brand Elements that may be confusingly similar to Snowflake's Brand Elements.

2.6. Data Processing and Transfer. Each party will act as a data controller (as that term is defined under the GDPR) with respect to personal data (as that term is defined in the GDPR) it receives as part of the SPN Program. Further, each party's processing of the data received from the other party, including the transfers of personal data relating to data subjects residing in the European Union (EU) or European Economic Area (EEA), the United Kingdom or Switzerland to countries not deemed to ensure an adequate level of data protection, shall be subject to the terms of the Data Sharing Addendum attached to this Agreement as Exhibit A.

3. CO-MARKETING

3.1. Brand Elements and Marketing Materials. Subject to the terms and conditions of this Agreement, each party (as the "licensing party") hereby grants to the other party (as the "licensed party") a limited, non-exclusive, worldwide, non-transferable, royalty-free right during the Term: (a) to use the licensing party's Brand Elements to identify it as a "partner" and for other reference purposes on the licensed party's website(s) and other sales and marketing collateral and (b) to use the licensing party's Brand Elements and Marketing Materials for the other marketing activities mutually approved by the parties in writing (if any). Partner's right to use Snowflake's Brand Elements and Marketing Materials extends only to those elements and materials associated with its then-current partner tier (for example, registered partners must not use the "Elite" tier badge). Upon request, the licensed party will provide samples of its use of the Brand Elements and Marketing Materials, and it will promptly cease any offending use of Brand Elements and Marketing Materials identified by the licensing party. For clarity, neither party is required to use the other party's Brand Elements and Marketing Materials.

3.2. Approvals and Restrictions. A licensed party must not, without the prior written permission of the licensing party: (a) modify, translate or create any derivative works of the licensing party's Marketing Materials (except that non-substantive format changes are permitted); (b) remove or obscure any Brand

Elements contained in the licensing party's Marketing Materials; or (c) publish, distribute or issue any joint product sheet, joint reference architectures, joint case study, joint press releases or other joint announcements. Partner's use of Snowflake's Brand Element and Marketing Materials will comply with Snowflake's then-current Snowflake Brand Guidelines (defined below). Snowflake's use of Partner's Brand Elements and Marketing Materials will comply with any reasonable brand and usage guidelines it receives in writing from Partner (if any).

4. CONDUCT AND RESPONSIBILITIES.

4.1. Unethical Conduct. In carrying out any activities pursuant to this Agreement or as an SPN Program partner, Partner shall not: (a) make any warranties, guarantees, or legal representations or commitments of any type on behalf of Snowflake or with respect to the Snowflake Technology (defined below); (b) describe Snowflake Technology in a manner inconsistent with Snowflake's Marketing Materials; or (c) violate any laws or engage in any deceptive, misleading, illegal or unethical practices.

4.2. Integrity in Sales Practices. Partner shall adhere to Snowflake's Business Partner Standards of Conduct (currently located at <https://www.snowflake.com/wp-content/uploads/2019/06/business-partner-standards-of-conduct.pdf> or such or such successor URL as may be designated by Snowflake). Further, Partner certifies that it shall not use unethical practices, or in cases of dealing with the government, violate 31 U.S.C. 1352 (concerning payments to influence federal transactions) or the Procurement Integrity Act (Subsection 27(a) of the Federal Procurement Policy Act, (42 U.S.C. 423) as amended by Section 814 of Public Law (101-189) to obtain information or to secure business for itself or others. Partner further agrees that while performing any activities under this Agreement, it shall comply with all applicable anti-bribery and anti-corruption laws and regulations, including but not limited to the U.K. Bribery Act 2010, the United States Foreign Corrupt Practices Act of 1977 (as amended pursuant to the 1988 Amendments and the International Anti-Bribery and Fair Competition Act of 1998) and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. Without limiting the generality of the foregoing obligation, Partner warrants that it has not and will not give, offer, or promise any payment or any item of value to: (i) any U.S. or non-U.S. government official, which shall include any person working for a state owned entity; (ii) any U.S. or non-U.S. political party official or political party; (iii) any candidate for a U.S. or non-U.S. political office; or (iv) any officer or employee of a public international organization (each, an "Official"), for the purpose of influencing any act or decision of these Officials in their official capacity to help obtain or retain business, or gain any unfair advantage. Partner represents and warrants that it will not retain any Official in connection with the performance of its activities hereunder.

4.3. Partner Data. Subject to the terms of this Agreement, Partner hereby grants to Snowflake a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify and display the Partner Data to provide the Partner Portal, to carry out applicable SPN Program Activities and to exercise Snowflake's rights and obligations under this Agreement or applicable law. Partner represents and warrants that: (a) it has provided any necessary notices and has sufficient rights in the Partner Data to allow Snowflake to use and process it as authorized under this Agreement (including as needed to permit cross-border transfers of personal data to Snowflake, if any) and (b) the Partner Data and its authorized processing by Snowflake will not infringe or

violate the intellectual property, publicity, privacy or other rights of any third party (including rights under Data Protection Laws). If Partner provides any prospects, leads or referrals to Snowflake, it further represents and warrants that it has provided all necessary notices and obtained all necessary consents to allow Snowflake, its Affiliates and Snowflake-authorized business partners to communicate with the applicable individuals for Snowflake's marketing, sales, and other business purposes. Partner shall notify Snowflake (via email sent to privacy@snowflake.com) within three business days of receiving a data subject request to exercise any rights under applicable Data Protection Laws.

4.4. Partner Services. To the extent Partner provides any of its own products or services to customers, including without limitation any proof of concepts for customers, Partner remains solely responsible for these products and services and its own relationships and agreements related to the same. Any use by Partner of a customer's Snowflake Service account is subject to such customer's approval and its applicable agreement with Snowflake.

4.5. Responsibility for Personnel. Partner will at all times be responsible for all actions or omissions of Partner Personnel in connection with this Agreement (including for their use of Training Materials and other resources and for their activities in connection with the SPN Program) and for anyone accessing the Partner Portal with its credentials. Partner represents and warrants that: (a) it and its Partner Personnel have the required power and authority to enter into this Agreement and to perform its obligations hereunder and (b) the execution of this Agreement and performance of its obligations hereunder do not and will not violate any other agreement to which it is a party. Partner and Partner Personnel must use the Partner Portal in accordance with Snowflake's Acceptable Use Policy (currently available at <https://www.snowflake.com/legal/>)

4.6. Affiliates. Each of Partner's Affiliates may join the SPN Program separately by signing up separately through the Partner Portal. If Partner permits any of its Affiliates to access the Partner Portal or participate in any SPN Program tiers, benefits or activities (including use of Training Materials and other resources) using Partner's SPN membership, then Partner (i) hereby binds that Affiliate to this Agreement and represents and warrants that it has the power and authority to do so and (ii) will be jointly and severally responsible and liable with its Affiliate for compliance with the terms and conditions of this Agreement and the Guidelines. In such latter case, Snowflake may terminate participation by any Partner Affiliate (or its personnel) at any time in its sole discretion.

5. PAYMENTS.

Registration for the SPN Program is free but Partner may choose to enroll in optional SPN Program tiers, activities and benefits that may require payment of fees. Unless otherwise specified in the applicable Guidelines, Partner will pay applicable fees through the Partner Portal and authorizes Snowflake to charge these fees to the credit card provided. If Snowflake invoices Partner for fees, unless otherwise set forth in the applicable Guidelines or order form(s), Partner will make payment in U.S. dollars to be paid within thirty (30) days from the date of Snowflake's invoice. Partner will be responsible for all taxes, withholdings, duties and levies in connection with the SPN Program (excluding taxes based on the net income of Snowflake). If Snowflake has the legal obligation to pay or collect taxes for which Partner is responsible under this Section, Snowflake will invoice Partner and Partner will pay that amount unless Partner provides

Snowflake with a valid tax exemption certificate authorized by the appropriate taxing authority. Unless otherwise expressly stated in the applicable Guidelines, all fees are non-refundable and non-creditable and payment obligations are non-cancellable once incurred. Partner waives any rights it may have to set-off, net, recoup, deduct, withhold, suspend or otherwise condition payment of fees. Any credits, discounts or other payments by Snowflake, such as referral commissions, are subject to the payment provisions of the applicable Guidelines.

6. INTELLECTUAL PROPERTY RIGHTS.

Except for the licenses expressly provided in this Agreement, each party retains all right, title and interest in and to its Brand Elements, Marketing Materials and Confidential Information. Any goodwill associated with the use of Brand Elements and Marketing Materials will inure to the licensing party's benefit. Snowflake or its suppliers shall retain all right, title and interest (including all patent, copyright, trademark, trade secret and other intellectual property rights) in and to Snowflake's products, programs and services (including the SPN Program, Partner Portal, Training Materials and the Snowflake Service), any and all related or underlying technology, software, features, content and documentation, and any derivative works, modifications, or improvements of any of the foregoing, including as may incorporate any Feedback (collectively, "**Snowflake Technology**"). This Agreement does not grant Partner any licenses to Snowflake Technology except for the limited licenses to the Partner Portal and Training Materials as expressly stated herein. Notwithstanding anything to the contrary herein, Snowflake may freely use and incorporate into Snowflake Technology any suggestions, ideas or other feedback provided by Partner ("**Feedback**") without any obligation, payment, or restriction based on intellectual property rights or otherwise.

7. CONFIDENTIAL INFORMATION.

Each party (as "**Receiving Party**") will protect the Confidential Information of the other party (as "**Disclosing Party**") using the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but not less than reasonable care). The Receiving Party will: (i) not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement and (ii) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of its employees, agents and contractors who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections not materially less protective than those herein. If Receiving Party is required by law or court order to disclose Confidential Information, then Receiving Party shall, to the extent legally permitted, provide Disclosing Party with advance written notification and cooperate in any effort to obtain confidential treatment of the Confidential Information. The Receiving Party acknowledges that disclosure of Confidential Information may cause substantial harm for which damages alone may not be a sufficient remedy, and therefore that upon any such disclosure by the Receiving Party, the Disclosing Party will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law.

8. INDEMNITY.

8.1. Indemnification. Each party (as the "**Indemnifying Party**") will defend the other party, its Affiliates, and their officers, directors, employees and representatives (each, an "**Indemnified Party**") against any third-party claim that the

Indemnifying Party's Brand Elements or Marketing Materials infringe such third party's copyright, trademark or publicity rights, and will indemnify and hold harmless the Indemnified Parties from and against any resulting damages, fees (including attorneys' fees), liabilities and costs awarded against the Indemnified Party or agreed to in a settlement by the Indemnifying Party. Further, Partner (as the Indemnifying Party) will defend Snowflake's Indemnified Parties from and against any third party claims arising from a breach or alleged breach of Section 4 (Conduct and Responsibilities), and will indemnify and hold harmless Snowflake's Indemnified Parties from and against any resulting damages, fees (including attorneys' fees), liabilities and costs awarded against Snowflake's Indemnified Parties or agreed to in a settlement by the Indemnifying Party.

8.2. Procedures. The Indemnifying Party's obligations are subject to receiving: (a) prompt written notice of a claim (but in any event notice in sufficient time for the Indemnifying Party to respond without prejudice); (b) the exclusive right to control and direct the investigation, defense, and settlement of a claim; and (c) all reasonable cooperation required from the Indemnified Party at the Indemnifying Party's expense. The Indemnifying Party may not settle any claim without the prior written consent of the Indemnified Party if the settlement requires the Indemnified Party to admit fault, pay any amounts (other than payment covered by the Indemnifying Party) or take or refrain from taking any action (other than to cease using the allegedly infringing materials). An Indemnified Party may participate in the defense of any claim by counsel of its own choosing, at its own cost and expense. In the event a claim is made or threatened, the Indemnified Party will cease use of any allegedly infringing Brand Elements or Marketing Materials at the Indemnifying Party's written request.

9. WARRANTY DISCLAIMER.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, EXCEPT FOR THE EXPRESS WARRANTIES IN THIS AGREEMENT, EACH PARTY HEREBY DISCLAIMS (ON BEHALF OF ITSELF AND ITS LICENSORS AND SUPPLIERS) ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SNOWFLAKE'S PARTNER PORTAL, TRAINING MATERIALS AND ANY OTHER SNOWFLAKE TECHNOLOGY ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS WITHOUT WARRANTIES OF ANY KIND. SNOWFLAKE DOES NOT WARRANT OR GUARANTEE THAT THE PARTNER PORTAL (INCLUDING ANY OF ITS CONTENT), TRAINING MATERIALS AND OTHER SNOWFLAKE TECHNOLOGY WILL MEET PARTNER'S REQUIREMENTS OR WILL BE UNINTERRUPTED, ACCURATE, UP TO DATE, TIMELY, SECURE OR ERROR FREE. NO STATEMENT OF SNOWFLAKE OR ANY OF SNOWFLAKE'S DIRECTORS, OFFICERS, SHAREHOLDERS, EMPLOYEES, CONTRACTORS, AGENTS, REPRESENTATIVES AND AFFILIATES SHALL CREATE ANY WARRANTY OTHER THAN THOSE EXPRESSLY CONTAINED IN THIS AGREEMENT. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES. HOWEVER, ANY STATUTORILY REQUIRED WARRANTIES, IF ANY, IS HEREBY LIMITED TO THE SHORTEST PERIOD AND TO THE MAXIMUM EXTENT PERMITTED BY LAW.

10. LIMITATION OF LIABILITY.

10.1. Exclusions and Limitations. TO THE MAXIMUM EXTENT PERMITTED BY LAW, AND EXCEPT FOR EXCLUDED CLAIMS (DEFINED BELOW), IN NO EVENT WILL EITHER PARTY OR ITS RESPECTIVE EMPLOYEES, OFFICERS, DIRECTORS, REPRESENTATIVES, LICENSORS, SUPPLIERS AND AGENTS BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, INDIRECT, COVER, RELIANCE, EXEMPLARY OR PUNITIVE DAMAGES OF ANY KIND (INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF BUSINESS OR PROFITS), EVEN IF A PARTY HAS BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY LAW, AND EXCEPT FOR EXCLUDED CLAIMS, EACH PARTY'S AND ITS RESPECTIVE EMPLOYEES', OFFICERS', DIRECTORS', REPRESENTATIVES', LICENSORS', SUPPLIERS' AND AGENTS' LIABILITY ARISING UNDER OR RELATING TO THIS AGREEMENT SHALL NOT EXCEED IN AGGREGATE (FOR ANY AND ALL CLAIMS AND THEORIES OF LIABILITY) ONE THOUSAND U.S. DOLLARS (\$1000.00) OR, IF GREATER, THE AMOUNT PAID OR PAYABLE UNDER THIS AGREEMENT BY A PARTY HEREUNDER IN THE TWELVE (12) MONTH PERIOD PRECEDING A CLAIM. THE EXISTENCE OF MORE THAN ONE CLAIM SHALL NOT ENLARGE THESE LIMITS.

10.2. Exceptions. "EXCLUDED CLAIMS" MEANS CLAIMS ARISING FROM: (I) A PARTY'S EXPRESS DEFENSE AND INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT; (II) BREACH BY A PARTY OF SECTION 7 (CONFIDENTIAL INFORMATION) (BUT EXCLUDING CLAIMS ARISING FROM UNAUTHORIZED LOSS, ALTERATION, USE OR DISCLOSURE OF, OR ACCESS TO, PARTNER DATA); (III) A PARTY'S INFRINGEMENT OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS PROVIDED PURSUANT TO THIS AGREEMENT; (IV) FRAUD; OR (V) DEATH, PERSONAL INJURY OR TANGIBLE PROPERTY DAMAGE TO THE EXTENT CAUSED BY A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

10.3. Other Terms. EACH PARTY ACKNOWLEDGES AND AGREES THAT THIS SECTION 10 IS A FUNDAMENTAL BASIS OF THE BARGAIN AND A REASONABLE ALLOCATION OF RISK BETWEEN THE PARTIES AND WILL SURVIVE AND APPLY TO ANY CLAIMS BY A PARTY OR ANY THIRD PARTY ARISING OUT OF OR RELATED TO THIS AGREEMENT, REGARDLESS OF THE FORM OF ACTION (WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE), EVEN IF ANY LIMITED REMEDY IN THIS AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE. SECTION 10.1 WILL ALSO APPLY TO SNOWFLAKE'S AFFILIATES, AND THEIR EMPLOYEES, OFFICERS, DIRECTORS, REPRESENTATIVES, LICENSORS, SUPPLIERS AND AGENTS AND TO CLAIMS BETWEEN THE PARTIES ARISING UNDER THE DATA SHARING ADDENDUM.

11. TERM AND TERMINATION.

This Agreement is effective as of the Effective Date and will have an initial term of twelve (12) months, unless earlier terminated in accordance with this Section. This Agreement will automatically renew for additional, successive twelve (12) month terms unless either party gives the other written notice of non-renewal at least thirty (30) days prior to the expiration of the then-current term. The initial term and any renewal terms are the "Term" of this Agreement. Either party may terminate this Agreement for any reason or no reason upon thirty (30) days written notice to the

other party and upon five (5) days written notice upon material breach by the other party. Upon termination or expiration of this Agreement, Partner agrees to cease SPN Program activities hereunder and each party must: (a) cease any ongoing co-marketing activities, including any subsequent use of the licensing party's Brand Elements and Marketing Materials and (b) at the Disclosing Party's request, return and/or destroy the Disclosing Party's Confidential Information, Brand Elements and Marketing Materials and certify destruction of the same. Notwithstanding the foregoing, the Receiving Party may retain backups of these items in order to comply with applicable law or its record keeping and retention policies, and these backups shall remain subject to Section 7 (Confidential Information). Without limiting its other available remedies, Snowflake may revoke or suspend access to the Partner Portal to address security, integrity or availability issues or in the event of a breach or suspected breach of this Agreement or Snowflake's Acceptable Use Policy.

12. GENERAL TERMS

12.1. Entire Agreement. This Agreement (which includes the Guidelines, the Data Sharing Addendum and the India Country Terms, only as applicable) is the complete agreement between the parties relating to the subject matter hereof and supersedes and cancels all previous written and oral agreements and communications relating to such subject matter. The Guidelines, Data Sharing Addendum and India Country Terms are incorporated by reference into this Agreement. If you previously entered into a Solution Partner Alliance Agreement, Partner Access Agreement (For Technology Partners), Marketing and Referral Agreement or Referral Program Agreement, please note that these legacy agreements do not govern the SPN Program and have been terminated.

12.2. Non-Disparagement. During the Term of this Agreement, neither Snowflake nor Partner will make any public statement (whether written or oral) that is intended to criticize or disparage the other party or any of its Affiliates. For clarity, the foregoing shall not limit a party's ability to bring legal claims before a court, regulator or arbitrator of competent jurisdiction

12.3. Dispute Resolution. Each party agrees that before it seeks any form of legal relief it shall provide written notice to the other party of the specific issue(s) in dispute with a reference to the relevant provisions of the contract between the parties which are allegedly being breached. Within thirty (30) days after such notice, knowledgeable executives of the parties shall hold at least one meeting (in person or by video- or tele- conference) for the purpose of attempting in good faith to resolve the dispute. The parties agree to maintain the confidential nature of all disputes and disagreements between them, including but not limited to informal negotiations, mediation or arbitration, except as may be necessary to prepare for or conduct these dispute resolution procedures or unless otherwise required by law or judicial decision. Notwithstanding the foregoing, the dispute resolution procedures in this Section shall not prevent a party from seeking provisional remedies to address claims of misappropriation or infringement of its intellectual property, trade secrets or Confidential Information.

12.4. Governing Law; Jurisdiction and Venue. This Agreement will be governed by the laws of Delaware and the United States without regard to conflict of laws provisions thereof, and without regard to the United Nations Convention on the International Sale of Goods. The exclusive jurisdiction and venue for actions related to the subject matter hereof will be the State and federal courts located in New Castle County, Delaware, and

both parties hereby submit to the personal jurisdiction of such courts.

12.5. Assignment. This Agreement will bind and inure to the benefit of each party's permitted successors and assigns. Neither party may assign this Agreement without the advance written consent of the other party, except that either party may assign this Agreement in its entirety in connection with a merger, reorganization, acquisition, or other transfer of all or substantially all of such party's assets or voting securities to such party's successor and Snowflake may assign this Agreement in its entirety to any Affiliate. Each party shall promptly provide notice of any such assignment. Any attempt to transfer or assign this Agreement except as expressly authorized under this Section will be null and void. The foregoing notwithstanding, Partner is prohibited from assigning this Agreement to any Snowflake competitor.

12.6. Severability; Interpretation. If a court of competent jurisdiction holds any provision of this Agreement to be unenforceable or invalid, that provision will be limited to the minimum extent necessary so that this Agreement will otherwise remain in effect. Section headings are inserted for convenience only and shall not affect the construction of the Agreement. Unless otherwise specified, "including" (and its variants) means "including without limitation" (and its variants) and any examples are intended to be illustrative, not limiting

12.7. Notice. Any notice or communication required or permitted under this Agreement will be in writing to the parties and will be deemed to have been received by the addressee: (a) if given by hand, immediately upon receipt; (b) if given by overnight courier service, the first business day following dispatch; (c) if given by registered or certified mail, postage prepaid and return receipt requested, the second business day after such notice is deposited in the mail; or (d) if given by email, immediately upon receipt. Any email notices related to this Agreement (including any termination) must be sent: (a) if to Snowflake, to the Snowflake addresses provided during enrollment with a copy to legalnotices@snowflake.com and (b) if to Partner, to the Partner's primary point of contact specified on the SPN Portal. Notwithstanding the foregoing, notices related to any legal claims against Snowflake (including without limitation breach or indemnity) may not be given via email.

12.8. Amendments; Waivers. From time to time, Snowflake may update this Agreement (including the Guidelines) and other policies and terms referenced herein. Partner's access to the Partner Portal and continuing participation in the SPN Program will be subject to any amendments. While Snowflake will make a commercially reasonable effort to notify Partner of material changes to this Agreement or the Guidelines through communications via the Partner Portal, email or other means, absence of notification does not relieve Partner of the obligation to monitor all changes, nor does it limit the enforceability of such updates. If Partner does not agree to updated terms, Partner must cease its participation in the SPN Program (including access to the Partner Portal and its content) and may terminate this Agreement as set forth above. Except as otherwise specified in this Section, any other amendment must be in writing signed by both parties. No waiver will be implied from conduct or failure to enforce or exercise rights under this Agreement, nor will any waiver be effective unless in a writing signed by a duly authorized representative on behalf of the party claimed to have waived.

12.9. Third Party Beneficiaries. There are no third-party beneficiaries under this Agreement except as otherwise expressly stated herein.

12.10. Force Majeure. Neither party will be liable to the other for any delay or failure to perform any obligation under this Agreement if the delay or failure results from any cause beyond such party's reasonable control, including acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism, or war.

12.11. Export Control. Each party agrees to comply with all applicable export and import laws and regulations of the United States and other applicable jurisdictions. Without limiting the foregoing, (i) each party represents and warrants that it is not listed on and will not engage with any U.S. government list of prohibited or restricted parties or located in (or a national of) a country that is subject to a U.S. government embargo or that has been designated by the U.S. government as a "terrorist supporting" country, (ii) each party will not (and will not permit any customer or third parties to) access or use any Snowflake Technology in violation of any U.S. export embargo, prohibition or restriction and (iii) Partner will not provide Snowflake with any Partner Data that contains information that is controlled under the U.S. International Traffic in Arms Regulations.

12.12. Relationship of Parties. Partner and Snowflake perform this Agreement as independent contractors. Notwithstanding the use of the term "partner," this Agreement does not create a partnership, joint venture, agency, fiduciary, or employment relationship. Each party is solely responsible for its expenses and costs of performing under this Agreement and for supervising, managing, contracting, directing, procuring, performing or causing to be performed its obligations under this Agreement, unless otherwise agreed upon in writing by the parties. Neither party's employees or contractors will be eligible for any compensation or benefits from the other party. Each party agrees that with respect to its own employees and contractors, it is solely responsible for: (i) payment of all applicable wages, incentives, compensation and required benefits to those individuals (including any unemployment insurance, workers' compensation, disability benefits and other required insurance); (ii) withholding, reporting and paying applicable employment-related taxes, including income withholding taxes, as required; and (iii) complying with any related applicable laws, including those regarding payment of wages, taxes, background checks, and eligibility for or entitlement to any required insurance, incentive, compensation or other benefits. Nothing set forth in this Agreement shall be construed to create the relationship of principal and agent between Partner and Snowflake. Neither party shall act or attempt to act or represent itself, directly or by implications, as an agent of the other or in any manner assume or create, or attempt to assume or create, any obligation on behalf of, or in the name of, the other party.

12.13. Survival. The following Sections will survive any expiration or termination of this Agreement: 1 (Partner Program), 4 (Conduct and Responsibilities), 5 (Payments), 6 (Intellectual Property Rights), 7 (Confidential Information), 8 (Indemnity), 9 (Warranty Disclaimers), 10 (Limitation of Liability), 11 (Term and Termination), 12 (General), 13 (Definitions), Exhibit B to the extent applicable, and any applicable provisions contained in the Guidelines that by their terms are intended to survive.

12.14. Counterparts. This Agreement may be entered into electronically and/or executed in counterparts, each of which will be deemed an original and all of which together will be considered one and the same agreement.

12.15. Indian entities. The terms of Exhibit B - India Country Terms, shall apply as applicable to Partner and/or its participating Affiliate(s) with a contracting entity located in India.

13. DEFINITIONS.

"Affiliate" means any entity that is controlled by, in control of, or is under common control with a party to this Agreement, where "control" means either the power to direct the management or affairs of the entity or ownership of 50% or more of the voting securities of the entity.

"Brand Elements" means a party's trademarks, service marks, names and logos.

"Confidential Information" means information identified at the time of disclosure as confidential or that should be reasonably known by the Receiving Party to be confidential based on its content and the circumstances of its disclosure. The Partner Portal (including its content), Training Materials and other Snowflake Technology are Snowflake's Confidential Information with no marking or further designation required. Confidential Information does not include information that the Receiving Party can document: (i) was rightfully in its possession or known to it prior to receipt of the Confidential Information; (ii) is or has become public knowledge through no fault of the Receiving Party; (iii) is rightfully obtained by the Receiving Party from a third party without breach of any confidentiality obligation; or (iv) is independently developed by the Receiving Party without use of such information.

"Data Protection Laws" means all data protection and privacy laws and regulations applicable to the respective party in its role in the processing of personal data under the Agreement, including, where applicable, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR") and the California Consumer Privacy Act of 2018 ("CCPA") and its regulations.

"Guidelines" means the Snowflake Partner Network Program Guide, the Referral Program Terms and the additional guidelines, terms and policies posted on the Partner Portal that describe and apply to specific SPN Program benefits, activities and/or tiers.

"Marketing Materials" means the images, documentation, collateral, case studies and similar materials that a licensing party may provide for use as part of any marketing activities under this Agreement. In the case of Snowflake, the term includes the collateral and materials available in the Partner Portal that are expressly designated by Snowflake as "For Customer Use."

"Partner Data" means the data or content that is provided by Partner to Snowflake in connection with the SPN Program, including Partner Personnel's account data, prospect, lead or referral information submitted by Partner, and content submitted to or posted on the Partner Portal.

"Partner Personnel" means Partner's and its Affiliate's employees, agents and contractors.

"Partner Portal" means Snowflake's partner portal for the SPN Program, currently located at www.snowflake.com/SPN.

"Referral Program Terms" means the Referral Program Terms located in the Partner Portal, which governs Snowflake's referral program.

“Snowflake” means the Snowflake entity specified by the chart located at <https://www.snowflake.com/legal/snowflake-contracting-entities/> in effect on the Effective Date.

“Snowflake Partner Network Program Guide” means the program guide posted on the Partner Portal that provides an overview of the Snowflake Partner Network program and additional tiers, benefits and requirements.

“Snowflake Service” means Snowflake’s cloud-based software-as-a-service solutions and related software.

“Snowflake Brand Guidelines” means Snowflake’s Branding Guidelines (currently available at <https://www.snowflake.com/brand-guidelines/>), Partner Content Guidelines (currently located within the Partner Portal) and other reasonable usage guidelines Snowflake may provide in writing to Partner.

“SPN Training Materials” means Snowflake’s then-current training and enablement materials made available through the Partner Portal, including sales and technical enablement materials and similar training content posted on the Partner Portal. For clarity, materials expressly designated by Snowflake as “For Customer Use” are considered Snowflake’s Marketing Materials, not Training Materials.

“Training Class Materials” means training materials and course content made available to Partner Personnel as part of a Snowflake training class.

“Training Materials” means the SPN Training Materials, Training Class Materials and similar Snowflake training content.

“Training SOW” means Snowflake’s then-current statement of work for training classes made available at <https://www.snowflake.com/legal/snowflake-sows/> (or such subsequent URL designated by Snowflake).

Other terms are defined in the main body of this Agreement, the Data Sharing Addendum or in the Guidelines.

EXHIBIT A - SPN DATA SHARING ADDENDUM

The following terms and conditions of this Data Sharing Addendum (the "**DSA**") are entered into in connection with the Snowflake Partner Network (SPN) Program Agreement (the "**Agreement**") by and between **Snowflake** and **Partner**, as each party is defined in the Agreement, where each party will act as a Controller, this DSA addresses the obligations for the processing of Personal Data (as defined below) processed in connection with such activities. Snowflake and Partner agree that notwithstanding anything to the contrary in the Agreement, including an integration clause, this DSA is hereby incorporated into and made an essential part of the Agreement.

AGREEMENT

1. DEFINITIONS

- 1.1 "**Affiliate**" means any entity that is directly or indirectly controlled by, controlling or under common control with an entity. "**Control**" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
- 1.2 "**Applicable Privacy Laws**" means those data protection and privacy laws and regulations worldwide applicable to the Personal Data in question, including, where applicable, European Data Protection Laws and Applicable State Privacy Laws.
- 1.3 "**Applicable State Privacy Law(s)**" shall mean individually and collectively, as applicable, those laws and regulations of the states within the United States that govern the transfer, sharing or sale to a third party of the personal information or personal data of consumers or individuals (as such transfers and data are defined in the applicable law), that are currently in effect or that become effective in the future, including, but not limited to, the California Consumer Privacy Act of 2018 ("**CCPA**") as updated by the California Privacy Rights Act of 2020 ("**CPRA**"), the Colorado Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act, and in each case, any amendments, final regulations, and successor legislation.
- 1.4 "**Business Contact Data**" means contact information relating to the Disclosing Party's representatives that the Receiving Party Processes for the purposes of (i) invoicing, billing and other business inquiries; and/or (ii) contract management.
- 1.5 "**Data Privacy Framework**" or "**DPF**" means (as applicable) the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework self-certification programs as operated by the U.S. Department of Commerce, and their respective successors.
- 1.6 "**DPF Principles**" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as may be amended, superseded, or replaced from time to time.
- 1.7 "**Europe**" means the European Economic Area and its Member States, the United Kingdom and Switzerland.
- 1.8 "**European Data Protection Laws**" means the applicable data protection and privacy laws and regulations of Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); (iii) the GDPR as it forms part of United Kingdom law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); and (iv) any national Applicable Privacy Laws made under or pursuant to (i) and (ii).
- 1.9 "**Personal Data**" means any data that the Disclosing Party shares with the Receiving Party that relates to an identified or identifiable natural person ("**data subject**") and/or that is deemed personal data, personal information, or personally identifiable information under Applicable Privacy Laws, including Business Contact Data.
- 1.10 "**Restricted Transfer**" means a transfer of Personal Data that is subject to European Data Protection Laws to a country that does not provide an adequate level of protection for Personal Data within the meaning of applicable European Data Protection Laws.
- 1.11 "**SCCs**" or "**Standard Contractual Clauses**" means together (i) the "**EU SCCs**", found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, or a successor website designated by the EU Commission, and (ii) the "**UK SCCs**" which are comprised of the EU SCCs as incorporated in and amended by the UK Addendum (as each may be updated, amended or superseded from time to time).
- 1.12 "**Security Incident**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data.
- 1.13 "**UK Addendum**" means the International Data Transfer Addendum issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018, currently available at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>

- 1.14 The terms "**Controller**" and "**Processing**" (including Process, Processed, and Processes), shall have the respective meanings ascribed to them in Applicable Privacy Laws. If and to the extent that Applicable Privacy Laws do not define such terms, then the definitions given in European Data Protection Laws will apply.

2. SCOPE OF DSA AND PROCESSING ROLES

- 2.1 **Scope of DSA.** The parties acknowledge that either party (the "**Disclosing Party**") may provide or make available to the other party (the "**Receiving Party**") Personal Data, as described at **Annex 1**. The Receiving Party shall Process the Personal Data for the purposes described at **Annex 1.B** (the "**Permitted Purpose**"), unless otherwise required by applicable law. If the Receiving Party wishes to Process the Personal Data for a new or different purpose, it may do so provided that it obtains any necessary consent from the individuals concerned and carries out any additional acts as are necessary to ensure that the Processing of the Personal Data for the new or different purpose fulfils the requirements of Applicable Privacy Laws.
- 2.2 **Roles of the Parties.** Each party and any permitted Affiliate shall: (i) Process the Personal Data as an independent Controller; and (ii) comply with its obligations under Applicable Privacy Laws and this DSA with respect to its Processing of Personal Data. In no event shall the parties Process the Personal Data as joint controllers within the meaning of European Data Protection Laws.

3. GENERAL RESPONSIBILITIES

- 3.1 **Compliance with Law.** Except as otherwise expressly agreed under this DSA or otherwise in writing, each party shall be individually and separately responsible for complying with the obligations that apply to it as a Controller under Applicable Privacy Laws. In particular (and without limitation): (a) each Disclosing Party shall be responsible for complying with all necessary requirements under Applicable Privacy Laws to lawfully collect and subsequently disclose the Personal Data to the Receiving Party for the Permitted Purpose; (b) each Receiving Party shall be separately and independently responsible for complying with Applicable Privacy Laws in respect of its Processing of Personal Data that it receives from Disclosing Party; and (c) neither party shall knowingly perform its obligations under this DSA in such a way as to cause the other party to breach any of its obligations under Applicable Privacy Laws.
- 3.2 **Cooperation.** Each party shall provide reasonable assistance to the other party as may be required in order to enable each party to fulfill its responsibilities under Applicable Privacy Laws. In particular, in the event that the Disclosing Party receives any requests or complaints from data subjects or regulatory or judicial bodies relating to the disclosure of Personal Data to, or Processing of Personal Data by, the Receiving Party ("Correspondence"), it shall promptly inform the Receiving Party giving relevant details of the same and the parties shall cooperate reasonably and in good faith, as necessary, in order to respond to the Correspondence in accordance with Applicable Privacy Laws.
- 3.3 **Security.** The Receiving Party shall implement and maintain all appropriate technical and organizational security measures to protect Personal Data from Security Incidents including, at a minimum, the measures identified at Annex 2 ("**Security Measures**").
- 3.4 **Notice, Consent and Opt-Out.** Each party shall post and maintain a publicly accessible privacy notice that satisfies the requirements of Applicable Privacy Laws, including but not limited to transparency and information requirements. Notwithstanding the foregoing, the Disclosing Party shall be responsible for ensuring that it has obtained all necessary and valid consents and authorizations and provided such notice and opt-out mechanisms to data subjects as may be required under Applicable Privacy Laws to enable the Receiving Party to lawfully Process the Personal Data for the Permitted Purposes.

4. INTERNATIONAL TRANSFERS

- 4.1 **International Transfers.** The Receiving Party shall not Process or transfer any Personal Data in or to a territory other than the territory in which the Personal Data was collected (nor permit such data to be so Processed or transferred) unless it takes those measures necessary to ensure such Processing or transfer is in compliance with Applicable Privacy Laws.
- 4.2 **Transfer Mechanism.** To the extent that the transfer of Personal Data from the Disclosing Party to the Receiving Party is a Restricted Transfer, the Receiving Party shall ensure an adequate level of protection as required by European Data Protection Laws and the DPF Principles by complying with the following:
- (a) If the Receiving Party is self-certified to the Data Privacy Framework, the Receiving Party shall use the Data Privacy Framework to lawfully receive such Personal Data so long as it (i) provides at least the same level of protection for such Personal Data as is required by the DPF Principles, and (ii) promptly notifies the Disclosing Party if it can no longer meet its obligations under the DPF Principles.
 - (b) Alternatively, if European Data Protection Laws require that appropriate safeguards are put in place (for example, if the Receiving Party is not self-certified to the Data Privacy Framework, the Data Privacy Framework does not cover the Restricted Transfer, and/or the Data Privacy Framework is invalidated), the SCCs shall automatically be incorporated into this DPA and apply to the Restricted Transfer as set forth in Section 4.3.

- 4.3 **Standard Contractual Clauses (SCCs).** Subject to Section 4.2 above, the parties agree that the SCCs shall be incorporated by reference and form an integral part of this DSA as follows:
- (c) the Disclosing Party (acting on behalf of itself and any applicable Affiliates) shall be the "data exporter" and the Receiving Party and/or its Affiliates (as applicable) shall be the "data importer";
 - (d) Module One of the SCCs shall apply as set out in **Annex 1.B**, and the same shall apply with respect to Table 2 of the UK Addendum;
 - (e) in Clause 11 of the SCCs, the optional language shall be deleted;
 - (f) in Clause 17 of the SCCs, Option 1 shall apply and the SCCs shall be governed by the laws of the Netherlands. Part 2, Section 15(m) of the UK Addendum regarding Clause 17 of the EU SCCs shall apply with respect to the UK SCCs;
 - (g) in Clause 18(b) of the SCCs, disputes shall be resolved before the courts of the Netherlands. Part 2, Section 15(n) of the UK Addendum regarding Clause 18 of the EU SCCs shall apply with respect to the UK SCCs;
 - (h) the Annexes of the SCCs shall be populated with the relevant information set out at **Annex 1** and **Annex 2** to this DSA;
 - (i) in Table 4 of the UK Addendum, either party may terminate the UK Addendum prior to termination of the Agreement and the DSA; and
 - (j) for transfers from Switzerland and other countries that adopt the SCCs for transfers from their respective country, references in the SCCs shall be interpreted to include applicable terminology for those territories (e.g. 'Member State' shall be interpreted to mean 'Switzerland' for transfers from Switzerland).
- 4.4 The parties acknowledge that either party may disclose this DSA (and any other relevant privacy terms or agreements entered between the parties) to the US Department of Commerce, the Federal Trade Commission, European data protection authorities or any other judicial or regulatory body having competent jurisdiction over such party, such as US, EU, Swiss or UK judicial or regulatory bodies, in each case upon their request.
- 4.5 **Binding Corporate Rules ("BCRs").** Notwithstanding Section 4.2, if Snowflake or Partner has adopted BCRs that cover the transfer of Personal Data to a Third Country under this DSA, then the BCRs shall govern the applicable transfer of Personal Data.

5. GENERAL

- 5.1 Any claim or remedy a party may have against the other party or the other party's employees and agents arising under or in connection with this DSA (including the SCCs), whether in contract, tort (including negligence) or under any other theory of liability, shall to the maximum extent permitted by applicable law be subject to the limitations and exclusions of liability in the Agreement. In no event shall either party limit the rights or remedies available to any data subject under Applicable Privacy Laws or this DSA (including the SCCs, if applicable).
- 5.2 The rights and obligations in this DSA shall survive so long as the Receiving Party Processes Personal Data.
- 5.3 This DSA is the complete and exclusive statement of the mutual understanding of the parties with respect to its subject matter. In the event of any conflict or inconsistency between this DSA and the Agreement, the terms of this DSA shall prevail with respect to the Processing of Personal Data. In the event of any conflict or inconsistency between this DSA and the SCCs (if applicable), the parties agree that the terms of the SCCs shall prevail.
- 5.4 This DSA will be governed by and construed in accordance with the governing law and jurisdiction provisions set forth in the Agreement, unless otherwise required by Applicable Privacy Laws or as set forth in the SCCs (if applicable) pursuant Section 4.2(d) and 4.2(e) above.

ANNEX 1

DESCRIPTION OF PROCESSING

Annex 1.A: List of parties

- If Snowflake is sharing Personal Data with Partner, Snowflake is the data exporter and Partner is the data importer.
- If Partner is sharing personal data with Snowflake, Partner is the data exporter and Snowflake is the data importer.

Snowflake	
Data exporter / Data importer:	Data exporter when acting as the Disclosing Party / Data importer when acting as the Receiving Party
Name:	Snowflake as identified under the Agreement
Address:	Locations listed at: https://www.snowflake.com/legal/snowflake-contracting-entities/
Contact person's name, position and contact details:	Head of Privacy, privacy@snowflake.com
Data Protection Officer:	dpo@snowflake.com
Representative:	privacy@snowflake.com or Snowflake Computing Netherlands B.V., FOZ Building, Gustav Mahlerlaan 300-314, 1082 ME Amsterdam, Netherlands
Activities relevant to data transferred:	Relevant activities are described in Annex 1.B below.
Role (controller / processor):	Controller

Partner	
Data exporter / Data importer:	Data exporter when acting as the Disclosing Party / Data importer when acting as the Receiving Party
Name:	Partner as identified under the Agreement
Address:	As listed for Partner in their Partner Portal account.
Contact person's name, position and contact details:	Primary contact listed for Partner in their Partner Portal account.
Activities relevant to data transferred:	Relevant activities are described in Annex 1.B below.
Role (controller / processor):	Controller

Annex 1.B: Description of the transfer

Description	Controller
SCCs Module	Module One
Categories of data subjects:	<ul style="list-style-type: none"> • Employees, agents, advisors, contractors, freelancers of the Disclosing Party; • Business contacts and marketing leads of the Disclosing Party; • Attendees of events hosted by the Disclosing Party
Categories of personal data:	Identification and contact data (name, title, address, phone number, email address); employment details (employer, job title, geographic location, area of responsibility, affiliated organization, area of responsibility and industry).
Sensitive data transferred (if applicable):	N/A
Frequency of the transfer:	Continuous, in connection with Partner Programs under the Agreement
Subject matter / Nature of the transfer and further processing:	The subject matter of the transfer and further Processing is the Personal Data obtained by the Disclosing Party and provided to or made available to the Receiving Party.
Purpose(s) of the data transfer and further processing:	The parties are sharing Personal Data in connection with the SPN Program including the marketing or selling their respective products and services to mutual customers and prospective customers and identifying potential business opportunities (the "Permitted Purpose").

Period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	The Personal Data shall be retained for so long as it is required for the Permitted Purpose and in accordance with the Receiving Party's data retention practices.
---	--

Annex 1.C: Competent supervisory authority

For the purposes of the SCCs (if applicable)

- Where Snowflake is the data exporter, the competent supervisory authority is the supervisory authority of the Netherlands.
- Where Partner is the data exporter, the competent supervisory authority will be determined in accordance with the GDPR and/or Applicable Privacy Laws.

ANNEX 2 SECURITY MEASURES

Description of the technical and organizational security measures implemented by the Receiving Party (i.e., data importer).

The Receiving Party shall perform the following tasks and adhere to the following obligations in the Processing and storage of Disclosing Party Personal Data pursuant to the Agreement:

- 1. Additional Definitions.** The capitalized terms used but not defined herein shall have the meaning set forth in the Agreement. The following terms shall have the ascribed meaning when used herein:
 - a. **“Device(s)”** means any device, computer or system that stores, Processes, transfers, transmits or otherwise accesses Disclosing Party Personal Data.
 - b. **“Physical Facilities”** means those data center or office structures either owned or leased by Receiving Party and which house equipment controlled by Receiving Party and/or by Receiving Party’s support personnel in connection with the Permitted Purpose.
- 2. Information Security Program Requirements.** Receiving Party shall implement and maintain throughout the term the following information security safeguards to protect the Disclosing Party Personal Data provided to Receiving Party in connection with the Permitted Purpose:
 - a. Policies and Governance. Receiving Party shall have in effect and apply an information security program to protect Disclosing Party Personal Data. Such information security program will be consistent with industry standards and will be designed or otherwise sufficient to: (1) protect the security and confidentiality of Disclosing Party Personal Data; (2) protect against any anticipated threats or hazards to the security or integrity of Disclosing Party Personal Data; and (3) protect against unauthorized access to or use of Disclosing Party Personal Data that could result in substantial harm or inconvenience to Disclosing Party.
 - b. Network Security and Encryption. Receiving Party will safeguard the confidentiality and integrity of all Disclosing Party Personal Data being transmitted over any form of data network and maintain strong, industry-standard encryption techniques for all cases in which Disclosing Party Personal Data is transmitted over any public data network. Receiving Party’s Internet connections will be protected with dedicated, industry-recognized firewalls that are configured and managed consistent with industry standards. Receiving Party shall not make any internal or private Internet Protocol (IP) address publicly available or natively routed to the Internet. Mobile devices, laptop and desktop computers will not store Disclosing Party Personal Data unless the Disclosing Party agrees there is a business need for such storage; if agreement is reached, Disclosing Party Personal Data on mobile devices and laptops will be encrypted in the agreed instances.
 - c. Information Stewardship and Segregation. Receiving Party will designate an employee who is responsible for managing the use of the Disclosing Party Personal Data, including on any Devices. All Disclosing Party Personal Data will also be logically and/or physically segregated from other information so that it can be identified as Disclosing Party Personal Data. Receiving Party will maintain controls designed to provide adequate segregation of duties among personnel, including access to systems and networks.
 - d. Training and Awareness. Receiving Party shall require all personnel to participate in information security training and awareness sessions at least annually, and track completion of training for all personnel.
 - e. Identification, Authentication and Authorization. Each user of any Device will have a uniquely assigned user ID and password to enable individual authentication and such ID will remain confidential and be removed promptly upon termination or transfer of the individual. Authentication mechanisms will include authentication methods to protect user accounts from known attack methods commensurate with the level of access and the associated risks of potential unauthorized access. Appropriate level of authentication implemented shall be proportionate to the sensitivity of the data. Authorized personnel, including but not limited to privileged users, shall only have the level of access required to perform their job functions. All remote and wireless access to Disclosing Party Personal Data or Devices will use a multi-factor authentication process prior to being allowed connection to Receiving Party’s network.
 - f. Vulnerability Management. Receiving Party shall implement malware detection/scanning services and procedures designed to protect against malicious code and/or malware, and to prevent against transferring malicious code to Disclosing Party’s systems. Receiving Party will use security measures to protect Devices that house Disclosing Party Personal Data to reduce the risk of infiltration, hacking, and access penetration by or exposure to an unauthorized third party. All Devices and Receiving Party systems will be kept current with appropriate security-specific system patches. Receiving Party will perform or require the performance of penetration tests as least once annually to detect any vulnerabilities.
 - g. Intrusion, Detection and Prevention. Receiving Party will use security measures, including Intrusion Prevention System (IPS) and Intrusion Detection System (IDS), to protect telecommunications system(s) and any Device used to reduce the risk of infiltration, hacking, access penetration by or exposure to a third party by (i) protecting against intrusions; (ii) securing the

Devices; (iii) protecting against intrusions of operating systems or software; and (iv) maintaining IPS and IDS systems consistent with manufacturer's recommended practice.

- h. Physical Security. Receiving Party shall maintain a security function to grant, adjust, and revoke physical access to its Physical Facilities.
- i. Security Incidents. Receiving Party shall establish processes and procedures for identifying and responding to security violations and unusual or suspicious events and incidents to limit and mitigate damage to information assets and to permit identification and prosecution of violators. These processes and procedures will include the ability to collect, analyze, and preserve evidence in a forensically sound manner to support criminal proceedings if required. If Receiving Party becomes aware of any Security Incident, to the extent permitted by law or law enforcement authorities it will: (i) promptly notify Disclosing Party of the Security Incident; (ii) investigate the Security Incident and provide Disclosing Party with, to the extent known, detailed information about the Security Incident; and (iii) take commercially reasonable steps, to the extent reasonably feasible, to mitigate the effects and to minimize any damage resulting from the Security Incident.
- j. Personnel Security: Receiving Party shall conduct standard background screening on its employees and contractors that (a) access Disclosing Party's systems or (b) Process Disclosing Party's Personal Data.
- k. Change Management. Receiving Party shall maintain a documented change management program for Receiving Party systems.
- l. Third Party Risk Management. For Receiving Party's vendors that (a) access the Disclosing Party systems or Receiving Party systems, or (b) access, Process, or store Disclosing Party's Personal Data, Receiving Party shall maintain a vendor risk management program designed to ensure each such vendor maintains security measures consistent with, and complies with, Receiving Party's obligations herein.
- m. Contact for Notification. Notification of Security Incidents, if any, will be delivered to Disclosing Party's designated relationship manager or another agreed-upon designate, in accordance with the Agreement's notice provisions, and in the case of Snowflake to security@snowflake.com.
- n. Logging and Monitoring. Receiving Party will keep audit logs that capture access to Disclosing Party Personal Data, new user adds, attempts to change security configurations, system start up, back up and shut down, and invalid login attempts. Audit logs will be retained by Receiving Party in a protected state (i.e., encrypted or locked), for a minimum of one (1) year, with processes in place to review periodically to detect intrusions, unauthorized access, unintended activities, malicious software or attempts of these or other actions that could compromise the security of systems Processing Disclosing Party Personal Data.
- o. Law Enforcement Requests. If Receiving Party receives a request from any law enforcement or government authority for Personal Data first provided by Disclosing Party as a part of Disclosing Party Personal Data, Receiving Party will attempt to redirect the authority to Disclosing Party to directly request the Personal Data in question. In doing so, Receiving Party may provide Disclosing Party's contact details to the relevant authority for this purpose. If legally compelled to disclose such Personal Data to any law enforcement or government authority, Receiving Party will endeavor to notify Disclosing Party prior to making such disclosure or, if that is not possible, as soon as reasonably practicable afterward unless it is legally prohibited from doing so.

3. Additional Receiving Party Obligations.

- a. Compliance with Disclosing Party Instructions. Receiving Party will process Personal Data only in accordance with the Agreement.
- b. Correspondence, Inquiries, and Complaints. Receiving Party may disclose information as required by law, in response to regulatory matters, or in compliance with applicable self-regulatory guidelines.
- c. Receiving Party Personnel. Receiving Party personnel will only access and use Personal Data in accordance with the Agreement (for example, for the Permitted Purpose). Receiving Party personnel are required to maintain the confidentiality of any Personal Data first provided by Disclosing Party as a part of the Disclosing Party Personal Data that they may access.
- d. Subcontractors. Receiving Party may appoint third party subcontractors to assist it in the performance of the Permitted Purposes. Disclosing Party consents to Receiving Party's appointment of third-party subcontractors, provided that:
 - (i) such subcontractors follow a security program comparable to that set forth herein;
 - (ii) such subcontractors process Personal Data first provided by Disclosing Party as a part of the Disclosing Party Personal Data only for the purpose of assisting Receiving Party in performing the Permitted Purposes; and,
 - (iii) Receiving Party remains responsible for subcontractors' actions undertaken in furtherance of performing the Permitted Purposes; and (iv) to the extent that such subcontractors Process Personal Data first provided by Disclosing Party as a part of the Disclosing Party Personal Data, Receiving Party has taken such measures as

are necessary to ensure adequate protection for any Personal Data first provided by Disclosing Party as a part of the Disclosing Party Personal Data.

- e. Business Continuity Management: Receiving Party maintains emergency and contingency plans for all Physical Facilities in which Receiving Party information systems that provide critical systems are located. Receiving Party's redundant storage and its procedures for recovering data (if such backups are available) are designed to attempt to reconstruct Personal Data in its original state from before the time it was lost or destroyed.

4. Audits and Certifications.

- a. Right to Audit. Subject to Section 4.b. below, Disclosing Party may, not more than once every twelve (12) months, conduct audits and security risk assessments to assess Receiving Party's information security program during normal business hours and upon no less than fifteen (15) business days' prior written notice of such audit or assessment. In connection with any such audits, shall at all times comply with applicable law and those of Receiving Party's reasonable security procedures and confidentiality requirements provided to Disclosing Party in writing reasonably in advance of any such audit. In addition, Disclosing Party's right to audit Receiving Party shall be subject to each of the following: (i) an agreed-upon statement between Receiving Party and Disclosing Party of the scope of any such audit; and (ii) Receiving Party's ability to participate in the audit. Under no circumstances shall Disclosing Party have the right to audit, or otherwise access or view, Receiving Party Property or any of Receiving Party's databases.
- b. Certification. Alternatively, to subsection 4.a. above, subject to the appropriate non-disclosure agreement prior to release, and if requested in writing, Receiving Party may provide an industry-standard security certification, or third-party assessment report (e.g. SOC 2 Type II or ISO27001) to evidence the establishment and implementation of an information security program as set forth above in Section 2 (Information Security Program Requirements).
- c. Remediation. Receiving Party will make good faith, commercially reasonable efforts to remediate (i) any errors identified in an audit that could reasonably be expected to have a material adverse impact on the Disclosing Party Personal Data and (ii) material control deficiencies identified in the audit or assessment.

EXHIBIT B – INDIA COUNTRY TERMS

The following changes will be made to the Agreement as applicable to Partner's contracting entity located in India that transacts with SNFL Cloudtech India Private Ltd., and as applicable to the Partner's Affiliate contracting entity located in India that transacts with SNFL Cloudtech:

1. Section 5 (**Payments**) of the Agreement shall be deleted in its entirety and replaced with the following:

"Registration for the SPN Program is free but Partner may choose to enroll in optional SPN Program tiers, activities and benefits that may require payment of fees. Unless otherwise specified in the applicable Guidelines, Partner will pay applicable fees through the Partner Portal and authorize Snowflake to charge these fees to the credit card provided. If Snowflake invoices Partner for fees, unless otherwise set forth in the applicable Guidelines or order form(s), Partner will make payment in INR to be paid within thirty (30) days from the date of Snowflake's invoice. Partner will be responsible for all taxes, withholdings, duties and levies in connection with the SPN Program (excluding taxes based on the net income of Snowflake). If Snowflake has the legal obligation to pay or collect taxes for which partner is responsible for under this Section, Snowflake will issue a valid tax invoice to Partner and Partner will pay that amount unless Partner provides Snowflake in advance of execution of the order form or payment of the applicable fee with a valid tax exemption certificate authorized by the appropriate taxing authority. Taxes will not be deducted from payments to Snowflake, except if the Partner is required by Indian law to pay the Tax Deducted at Source ("TDS") on the fees. Partner is responsible for filing the proper tax forms, making the appropriate TDS payments to the tax authorities and promptly providing Snowflake with the withholding tax certificate. Partner will provide its applicable Goods and Services Tax Identification Number ("GSTIN") on the order form or payment of the applicable fee. Unless otherwise expressly stated in the applicable Guidelines, all fees are non-refundable and non-creditable and payment obligations are non-cancellable once incurred. Partner waives any rights it may have to set-off, net, recoup, deduct, withhold, suspend or otherwise condition payment of fees. Any credits, discounts or other payments by Snowflake, such as referral commissions, are subject to the payment provisions of the applicable Guidelines.

2. As applicable to Partner and its Affiliates order forms placed and fees paid by Partner and its Affiliates to Snowflake under the Agreement, a new Section 5.1 (**Snowflake Electronic Invoices**) shall be added under the Agreement to include the following language:

"Where applicable, Snowflake shall raise electronic invoices ("**E-invoice**") for the program fees and purchased services and upload the same on the Government of India portal in accordance with the laws of India. Snowflake will not accept any changes in an E-invoice which is recorded and reported (i) on the E-invoice portal maintained by the Government of India, or (ii) in the goods and services tax returns of Snowflake under the tax laws of India."

3. As applicable to referral fee and funding payments Snowflake makes to Partner and its Affiliates under the Agreement, a new Section 5.2 (**Partner Invoices**) shall be added under the Agreement to include the following language:

"Where applicable, Partner shall raise valid tax invoices, including electronic invoices, for the referral fees and funding amounts paid by Snowflake to Partner under this Agreement and upload the same to Government of India portal in accordance with the laws of India. Partner shall defend, indemnify and hold Snowflake harmless for Partner's failure to properly comply with the requirements of this section 5.2, including any resulting damages, fee (including attorneys' fees), liabilities and costs awarded against Snowflake and as may be agreed to in a settlement by Partner."

4. Section 12.4 (**Governing Law; Jurisdiction and Venue**) in the Agreement shall be deleted in its entirety and replaced with the following:

"This Agreement will be governed by the laws of India without regard to conflicts of law provisions thereof, and without regard to the United Nations Convention on Contracts for the International Sale of Goods. If there is a dispute between the parties as to matters covered by this Agreement, or the validity, enforceability or interpretation thereof (each, a "**Dispute**"), the Dispute shall be submitted to the Singapore International Arbitration Centre, with venue and seat of arbitration as Singapore. The arbitration should be conducted in English before a single arbitrator having experience in technology disputes. The award shall be final and binding and enforceable in any court of competent jurisdiction. The parties undertake and agree that all arbitral proceedings conducted with reference to this Section shall be kept strictly confidential and all information disclosed in the course of such arbitral proceedings shall be used solely for the purpose of those proceedings. The provisions of this Section shall not prevent either party from seeking immediate injunctive relief or to enforce an arbitration award in any court of competent jurisdiction. If the subject matter of a Dispute does not permit the parties to use the dispute resolution or arbitration procedures set forth herein or such dispute resolution or arbitration procedures are deemed unenforceable, then any such Dispute shall be subject to the jurisdiction and venue for actions related to the subject matter hereof will be the courts located in Bangalore, Karnataka, and both parties hereby submit to the personal jurisdiction of such courts. While the Snowflake entity contracting with Partner or the Partner Affiliate remains fully liable and responsible for all Snowflake obligations under this Agreement, the parties acknowledge that certain obligations under this Agreement may be fulfilled by other Authorized Snowflake Affiliates, including without limitation, Snowflake Inc."

5. The existing Section 12.11 (**Export Control**) in the Agreement deleted in its entirety and replaced with the following:

“Each party agrees to comply with all export and import laws and regulations, including without limitation, of India and the United States and other applicable jurisdictions. Without limiting the foregoing, (i) each party represents and warrants that it is not listed on and will not sell to any Indian government or U.S. government list of prohibited or restricted parties or located in (or a national of) a country that is subject to an Indian government or U.S. government embargo or that has been designated by the Indian or U.S. government as a “terrorist supporting” country, (ii) each party will not (and will not permit any customer or third parties to) access or use any Snowflake Service in violation of any Indian or U.S. export embargo, prohibition or restriction, and (iii) each party will not permit customers to submit to the Snowflake Service any information that is controlled under the U.S. International Traffic in Arms Regulations.”

6. Section 13 in the Agreement (**Definitions**) shall be amended to add in the following additional definitions:

“**Authorized Snowflake Affiliate**” means a Snowflake Affiliate identified as an “Authorized Snowflake Affiliate” under “Snowflake Sub-Processors and Affiliates” at <https://www.snowflake.com/legal/>.