DATA PROCESSING ADDENDUM

Snow and Third Party have entered into an Agreement under which each Party will process the other Party's and its Affiliates' Personal Data which may be subject to Data Protection Laws. This Data Processing Addendum ("**Addendum**") governs and regulates the processing of Personal Data in accordance with applicable law and is incorporated by reference into the Agreement.

The Parties agree that the terms as set out below supersede and replace any existing privacy and data protection terms pertaining to the processing of Personal Data pursuant to the Agreement, subject to Data Protection Laws.

For the avoidance of doubt, any reference to Snow or Third Party shall mean the relevant Snow Affiliate or Third Party Affiliate that is a signatory to the applicable order form, purchase order or statement of work ("SOW") which is entered into under the Agreement. Snow and Third Party may each act as a Controller or Processor under this Addendum.

BY SIGNING AN AGREEMENT THAT REFERENCES THIS ADDENDUM, THE PARTIES AGREE TO THE TERMS OF THIS ADDENDUM AND NO SIGNATURE IS REQUIRED BELOW. IF THIS ADDENDUM IS NOT REFERENCED IN THE AGREEMENT AND IS BEING EXECUTED SEPARATELY FROM THE AGREEMENT, THIS ADDENDUM SHALL BE LEGALLY BINDING AND EFFECTIVE AS OF THE DATE OF THE LAST SIGNATURE BELOW.

Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified in this Addendum, the terms of the Agreement shall remain in full force and effect. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. DEFINITIONS

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

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

1.1.2 "**Agreement**" means the agreement between Third Party and Snow under which a Party provides Services to the other Party.

1.1.3 "**Authorized Affiliate**" means any of Third Party's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement, but is not a "customer" as defined under the Agreement;

1.1.4 "**Business**" and "**Service Provider**" shall have the meanings given to them in the CCPA;

1.1.5 "**California Personal Information**" means Personal Data that is subject to the protection of the CCPA;

1.1.6 "**CCPA**" means the California Consumer Privacy Act (California Civil Code §§ 1798.100 et seq.), as amended by the California Privacy Rights Act, and its implementing regulations;

1.1.7 "**Customer**" means the Snow customer named in the Agreement together with its Authorized Affiliates;

1.1.8 "**Data Protection Laws**" means all laws and regulations, including laws and regulations of the United Kingdom, the European Union ("EU"), the European Economic Area ("EEA"), their member states and Switzerland applicable to the Processing of Personal Data under the Agreement and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.9 "**EEA**" means the European Economic Area and/or their member states;

1.1.10 "**EU GDPR**" means the EU General Data Protection Regulation (EU) 2016/679of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

1.1.11 "**GDPR**" means both UK GDPR and EU GDPR;

1.1.12 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

1.1.13 "**Sell**" shall have the meaning given in the CCPA;

1.1.14 "**Services**" means the services and other activities ordered or subscribed to by a Party pursuant to the Agreement;

1.1.15 "**Standard Contractual Clauses**" means the Information Commissioners Office ("ICO") International Data Transfer Agreement for the transfer of personal data from the UK and/or the ICO's International Data Transfer Addendum to EU Commission Standard Contractual Clauses and/or the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to Commission Implementing Decision (EU) 2021/914 and/or the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU, or such alternative clauses as may be approved by the European Commission or by the UK from time to time;

1.1.16 "**Subprocessor**" means any person or entity (including any third party and any Processor Affiliate but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor or any Processor Affiliate to process Personal Data on behalf of Processor in connection with the Agreement.

1.1.17 "**Third Party**" means a Customer, vendor or authorized partner of Snow under the applicable Agreement.

1.1.18 "**UK GDPR**" means Data Protection Act 2018 as amended or updated from time to time.

1.2 The terms "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Process**", "**Processing**", "**Processor**" and "**Supervisory Authority**" shall have the same meaning as in the UK GDPR or EU GDPR (as applicable), and their cognate terms shall be construed accordingly.

2. PROCESSING OF PERSONAL DATA

2.1 Processor will process Personal Data under the Agreement only as a processor acting on behalf of the Controller's lawful instructions.

2.2 Processor will only process Personal Data on behalf of and in accordance with Controller's documented instructions. Controller instructs Processor to process Personal Data for the following purposes: (a) as reasonably necessary for the provision of the Services and consistent with the Agreement; (b) processing initiated by Controller's end users in their use of the Services; and (c) to comply with other reasonable instructions provided by Controller via support ticket, email, or otherwise where such instructions are consistent with the terms of the Agreement.

2.3 The subject matter of the processing of Personal Data is the provision or use of the Services under the Agreement. Processor will process Personal Data for the duration of the Agreement, unless otherwise agreed between Processor and Controller in writing or as required by applicable law. The nature and purpose of Processor's processing of Personal Data is to perform or use the Services pursuant to the Agreement and as instructed by Controller in its use of the Services. The Personal Data processed may include but is not limited to the following categories of data subjects: Controller's end users, employees, contractors, suppliers, and vendors, and other third parties (who are natural persons). The Personal Data processed may include but is not limited to the following categories: name, title, localization data, identification data, email address, or phone number.

2.4 Controller shall, in its provision, use or receipt of the Services, transfer Personal Data in accordance with the requirements of Data Protection Laws including but not limited to providing any required notices and obtaining any required consents, including for the written processing instructions it gives to the Processor, and ensure that its instructions for the processing of Personal Data shall comply with Data Protection Laws. Controller retains control of its Personal Data and shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Controller acquired Personal Data. Controller takes full responsibility to keep the amount of Personal Data provided to Processor to the minimum necessary for the performance of the Services.

2.5 The Controller warrants that:

2.5.1 it has complied and will continue to comply with Data Protection Laws;

2.5.2 its instructions for the Processing of Personal Data shall at all times comply with Data Protection Laws;

2.5.3 all Personal Data has been and will continue to be collected and processed in accordance with the notice, consent and other requirements of Data Protection Laws (and where applicable, the collection and processing has been notified to the relevant authorities)

2.5.4 it has and will continue to have the right to transfer or provide access to the Personal Data to Processor and the Subprocessors for the permitted purpose and that such Processing by Processor and the Subprocessors will not breach Data Protection Laws;

2.5.5 its instructions to Processor in respect of the Processing of Personal Data are lawful and will not create legal or regulatory liability on the part of Processor or any Subprocessor if followed.

2.6. When the Processor processes California Personal Information in accordance with the instructions received from the Controller, the parties acknowledge and agree that the Controller is a Business and the Processor is a Service Provider for the purposes of the CCPA. The Parties agree that the Processor will process California Personal Information as a Service Provider strictly for the purpose of providing, supporting and improving the Processor's Services (the "Business Purpose") and otherwise only as permitted by the CCPA or as required by law. Further, the Processor (i) will not Sell any California Personal Information; and (ii) will not process California Personal Information outside of the direct business relationship between the Parties, unless required by applicable law. The Processor certifies that it understands the foregoing obligations and will comply with them.

3. PERSONNEL

Processor restricts its personnel from processing Personal Data without authorization (unless required to so by applicable law) and will ensure that any person authorized by Processor to process Personal Data has received training pertinent to the care and handling of Personal Data and is subject to an obligation of confidentiality. Processor shall take commercially reasonable steps to ensure the reliability of any Processor personnel engaged in the processing of Personal Data. Processor shall ensure that its access to Personal Data is limited to those personnel performing or receiving Services in accordance with the Agreement.

4. SECURITY

4.1 Processor shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the UK GDPR and EU GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

5. SUBPROCESSING

5.1 Controller authorizes (a) Processor to appoint its Affiliates as Subprocessors; and (b) Processor and its Affiliates to appoint third-parties as Subprocessors in connection with the provision of the Services. As a condition to appointing a third-party as a Subprocessor, Processor or an Affiliate of Processor will enter into a written agreement with each third-party Subprocessor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this Addendum (to the extent applicable to the Services provided by such third-party Subprocessor). Processor will be responsible for any acts and omissions of its Subprocessors that cause Processor to breach any of its obligations under this Addendum.

5.2 Processor may continue to use those Subprocessors already engaged by it as of the date of this Addendum, and will provide a list of such Subprocessors currently engaged by the Processor (such list for Snow is available at www.snowsoftware.com/legal/dataprotection) or is provided by Processor to Controller upon request.

5.3 If Third Party sends an email to dpo@snowsoftware.com with the subject "Subprocessor Notice", Snow shall send written notice to the requesting Third Party email address of the appointment of any new Subprocessor before authorizing any new Subprocessor to process Personal Data in connection with the provision of the applicable Services. Third Party shall notify Snow by sending an email to dpo@snowsoftware.com at least 30 days in advance before authorizing any new Subprocessor to process Personal Data in connection with the provision of the applicable Services. If, within 10 business days of receipt of that notice, Controller notifies Processor in writing of any objections to the proposed appointment:

5.3.1 Processor shall work with Controller in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and

5.3.2 where such a change cannot be made within 30 days from Processor's receipt of Controller's notice, notwithstanding anything in the Agreement, Controller may by written notice to Processor terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor.

6. DATA SUBJECT RIGHTS

6.1 Taking into account the nature of the processing, Processor shall assist Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligations, as reasonably understood by Controller, to respond to requests to exercise data

subject rights under the Data Protection Laws in respect to Personal Data ("**Data Subject Request**").

6.2 Processor shall (save for any opt-out requests):

6.2.1 promptly notify Controller if Processor receives a Data Subject Request;

6.2.2 not respond to a Data Subject Request except on the documented instructions of Controller or as required by applicable laws, in which case Processor shall to the extent permitted by applicable laws inform Controller of that legal requirement before responding to the Data Subject Request; and

6.2.3 to the extent Controller does not have the ability to address a Data Subject Request in relation to the Services, Processor shall, upon Controller's request, provide commercially reasonable efforts to assist Controller to the extent Processor is legally permitted to do so and the response is required under Data Protection Law. To the extent permitted by applicable law, Controller shall be responsible for any costs arising from Processor's provision of such assistance.

7. PERSONAL DATA BREACH

7.1 Processor shall notify Controller without undue delay upon Processor becoming aware of a Personal Data Breach affecting Personal Data which may require a notification to be made to a supervisory authority or data subject under Data Protection Law or which Processor is required to notify to Controller under Data Protection Law, providing Controller with sufficient information to allow Controller to meet any obligations to report or inform data subjects of the Personal Data Breach under Data Protection Law.

7.2 To the extent such Personal Data Breach is caused by a violation of this Addendum by Processor, Processor shall provide commercially reasonable cooperation and assistance in identifying the cause of such Personal Data Breach and take commercially reasonable steps to remediate the cause to the extent the remediation is within Processor's control.

8. IMPACT ASSESSMENT

Upon Controller's request, Processor shall provide reasonable assistance to Controller with any data protection impact assessments ("DPIA"), at Controller's cost, needed to fulfil Controller's obligations to carry out a DPIA (to the extent Controller does not otherwise have access to the relevant information, and to the extent such information is available to Processor), to allow the Controller to comply with its obligations in relation to data security and DPIA, and any related consultations under Data Protection Laws which may include prior consultations with supervising authorities or other competent data privacy authorities, which Controller reasonably considers to be required of it by Data Protection Law, in each case solely in relation to processing of Personal Data taking into account the nature of the processing and information available to Processor.

9. DELETION OR RETURN OF PERSONAL DATA

9.1 Upon expiration or termination of the Services involving the processing of Personal Data, Processor shall, upon Controller's request, and subject to any limitations described in the Agreement, return to Controller, or securely destroy, all Personal Data and demonstrate to Controller's satisfaction that Processor has taken such measures, unless applicable law prevents it from returning or destroying all or part of Personal Data. Processor shall preserve the confidentiality of any retained Personal Data and will only actively process such Personal Data after such date as required by applicable law and in accordance with this Addendum.

10. AUDIT RIGHTS

10.1 Processor shall provide Controller on request information necessary to demonstrate compliance with this Addendum and the processing of the Personal Data.

10.2 To the extent required under Data Protection Law, Controller may additionally request, subject to the confidentiality obligations set forth in the Agreement, an on-site audit of Processor's procedures relevant to the protection of Personal Data carried out by an independent auditor appointed by the Controller, or if Controller is not a competitor of Processor, a copy of a Subprocessor's then-current certification and audit, by notifying Processor in writing providing reasonable notice (minimum thirty (30) days). Before the commencement of any such on-site audit, Processor and Controller shall mutually agree upon the scope, timing, and duration of the audit. Any audit shall only encompass relevant sites. Access to Processor's sites shall be supervised and controlled, and during normal business hours and they shall use reasonable endeavours to minimise disruption while exercising the rights of audit set out in this clause. Controller shall notify Processor of the identity of any visiting independent auditors to ensure they have entered into appropriate confidentiality agreements beforehand, approved by Processor (such approval not to be unreasonably withheld or delayed).

10.3 Audits shall take place no more than once in any calendar year unless and to the extent that Controller

(acting reasonably and in good faith) has reasonable and demonstratable grounds to suspect any material breach of this DPA by Processor, in which case Controller and Processor will agree timescales for the audit. Costs of the audit, including appointment of the independent auditor, will be borne by Controller.

10.4 Processor shall be entitled to reasonable time to review and retain any audit report, prepared by independent auditor and to consult the independent auditor on the content, prior to the audit report being submitted to Controller. For avoidance of doubt, all audit information of Processor obtained by Controller or an independent auditor pursuant to any audit shall be maintained in confidence by Controller and its independent auditor and may not be disclosed to any third party, including, without limitation, any other agents or representatives of Controller except to the extent necessary to assert or enforce any of the Controller's rights under this DPA or is required to be disclosed by Data Protection Laws, by any supervisory authority or by a court or other authority of competent jurisdiction provided that, to the extent it is legally permitted to do so, it gives Processor as much notice of this disclosure as possible and, where notice of disclosure is not prohibited and is given in accordance with this clause, it takes into account the reasonable requests of Processor in relation to the content of this disclosure.

10.5 Neither the independent auditor nor Controller shall be permitted to perform penetration tests, vulnerability scans, or otherwise interrogate Processor's network or information technology systems.

10.6 In no circumstances shall Controller or the independent auditor have access to:

10.6.1 individual payroll and Processor's personnel files;

10.6.2 individual expenditure or records relating to Processor's business or its other clients, partners or suppliers;

10.6.3 Processor's confidential information or trade secrets;

10.6.4 Any of Processor's overhead costs; or

10.6.5 Processor's server rooms or IT systems.

10.7 Controller shall reimburse Processor for any time expended for any such on-site audit at the agreed rate, which shall be reasonable taking into account the resources to be expended by Processor. Controller shall promptly notify Processor with information regarding any non-compliance discovered during the course of an audit, and Processor shall use commercially reasonable efforts to address any confirmed non-compliance.

11. RESTRICTED TRANSFERS

11.1 Processor may transfer Personal Data from the UK or EEA to countries outside the EEA only if such transfer is required in connection with the Services and at least one of the following safeguards is implemented: (a) the transfer is subject to the terms set out in the Standard Contractual Clauses, (b) the transferee is located in a country that has been deemed to provide an adequate level of protection for Personal Data by the European Commission or ICO for the UK, or (c) the transfer is subject to an alternative recognised compliance standard for the lawful transfer of Personal Data outside the UK or EEA.

11.2 If Controller transfers Personal Data from the UK or EEA to a Processor entity located in a country which does not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws, the terms of the Standard Contractual Clauses shall apply to Controller as the "data exporter" and Processor as the "data importer", to the extent such transfers are subject to such applicable Data Protection Laws.

12. LIMITATION OF LIABILITY

12.1 Any claims brought under this Addendum will be subject to the same terms and conditions, including any exclusions and limitations of liability, set out in the Agreement, except that any limitations of liability will not apply, to the extent required by applicable law, with respect to any data subject rights under the Standard Contractual Clauses. Where no Agreement exists, liability is not addressed within the Agreement, or where this DPA is entered into as a standalone agreement, then Snow's liability shall be limited to an aggregate of six months fees paid, or £5000 whichever is greater. Neither party seeks to limit its liability for death or personal injury caused by a parties negligence, fraud or anything else no allowed to be limited by applicable law.

13. GENERAL TERMS

13.1 Nothing in this Addendum reduces Processor's obligations under the Agreement in relation to the protection of Personal Data or permits Processor to process (or permit the processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.2 Severability - If any provision or portion thereof of this Addendum is found to be invalid, unlawful, or

unenforceable to any extent, such provision of this Addendum will be enforced to the maximum extent permissible by applicable law so as to affect the intent of the Parties, and the remainder of this Addendum will continue in full force and effect. The Parties will negotiate in good faith an enforceable substitute provision for any invalid or unenforceable provision that most nearly achieves the intent and economic effect of such provision.

13.3 Notice - All notices and approvals shall be in writing and sent to the Parties address stated hereunder unless subsequently updated (notified in writing to the other Party), and shall be deemed to have been given upon: (i) personal delivery; (ii) the day of receipt, as shown in the applicable carrier's systems, if sent via nationally recognized express carrier; or (iii) the third business day after first class, postage prepaid, posting. All notices by Third Party must include a copy to: legal@snowsoftware.com.

13.4 Law and Jurisdiction - The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity. Where no such jurisdiction is stipulated, or this DPA is entered into as a standalone document, then the parties agree to submit to English law, and the exclusive jurisdiction of the English Courts.

The parties' authorized signatories have duly executed this Addendum:

(SIGNATURE IS ONLY REQUIRED IF THIS ADDENDUM IS NOT REFERENCED IN THE AGREEMENT)

THIRD PARTY		**SNOW SOFTWARE**	
Third Party Legal Name:	_____	*Snow Software Legal Name:*	_____
Signature:	_____	*Signature:*	_____
Date Signed:	_____	*Date Signed:*	_____
Print Name:	_____	*Print Name:*	_____
Title:	_____	*Title:*	_____
Address:	_____	*Address:*	_____
	_____		_____