Snowflake Customer Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of, and is subject to, the Master SaaS Agreement or other written or electronic terms of service or subscription agreement between the member of the Snowflake Group that is a party to such agreement ("**Snowflake**") and the legal entity defined as 'Customer' thereunder together with all Customer Affiliates who are signatories to an Order Form for their own Service Account pursuant to such agreement (collectively, for purposes of this DPA, "**Customer**") (such agreement, the "**Agreement**"). This DPA shall be effective on the effective date of the Agreement, unless this DPA is separately executed in which case it's effective on the date of the last signature ("**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions.

"**Account**" means Customer's account in the Service in which Customer stores and processes Customer Data.

"**Affiliate**" has the meaning set forth in the Agreement.

"**Authorized Affiliate**" shall mean a Customer Affiliate who has not signed an Order Form pursuant to the Agreement, but who is the Data Controller for the Customer Personal Data processed by Snowflake pursuant to the Agreement, for so long as such entity remains a Customer Affiliate.

"**California Consumer Privacy Act**" or "**CCPA**" means the California Consumer Privacy Act of 2018, as may be amended from time to time.

"**Customer Data**" has the meaning set forth in the Agreement.

"**Customer Personal Data**" means any Customer Data that is Personal Data.

"**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means an entity that Processes Personal Data on behalf of a Data Controller.

"**Data Protection Laws**" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law and the CCPA.

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

"**EU Data Protection Law**" means 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**").

"**Services**" means the generally available Snowflake software-as-a-service offering described in the Documentation and procured by Customer, and any other services provided by Snowflake under the Agreement, including but not limited to support and technical services.

"**Personal Data**" means any information, including opinions, relating to an identified or identifiable natural person and includes similarly defined terms in Data Protection Laws, including, but not limited to, the definition of "personal information" in the CCPA.

"**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

"**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

"**Processing**" shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination and "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Purposes**" shall mean (i) Snowflake's provision of the Services in accordance with the Agreement, including Processing initiated by Users in their use of the Services, and (ii) further documented, reasonable instructions from Customer agreed upon by the parties.

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

"**Snowflake Group**" means Snowflake Inc. and its Affiliates.

"Standard Contractual Clauses" means the Standard Contractual Clauses for Processors as approved by the European Commission in the form set out in Annex A**.**

"**Sub-processor**" means any third-party Data Processor engaged by a member of the Snowflake Group to Process Customer Personal Data.

2. Scope and Applicability of this DPA. This DPA applies where and only to the extent that Snowflake Processes Customer Personal Data on behalf of Customer as Data Processor in the course of providing the Services.

3. Roles and Scope of Processing.

3.1 **Role of the Parties**. As between Snowflake and Customer, Customer is either the Data Controller of Customer Personal Data, or if Customer is acting on behalf of a third-party Data Controller, then a Data Processor, and Snowflake shall Process Customer Personal Data only as a Data Processor acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined therein. To the extent any Service Data (as defined in the Agreement) is considered Personal Data under applicable Data Protection Laws, Snowflake is the Data Controller of such data and shall Process such data in accordance with the Agreement and applicable Data Protection Laws.

3.2 **Customer Instructions**. Snowflake will Process Customer Personal Data only for the Purposes. Customer shall ensure its Processing instructions are lawful and that the Processing of Customer Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. The parties agree that the Agreement (including this DPA) sets out Customer's complete and final instructions to Snowflake for the Processing of Customer Personal Data. Any Processing outside the scope of these instructions will require prior written agreement between Customer and Snowflake.

3.3 **Customer Affiliates.** Snowflake's obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions:

(a) No entity other than Customer may provide further Processing instructions to Snowflake and Customer must accordingly communicate any additional Processing instructions from its Authorized Affiliates directly to Snowflake;

(b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations in this DPA shall be considered the acts and/or omissions of Customer; and

(c) Authorized Affiliates shall not bring a claim directly against Snowflake. If an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against Snowflake ("**Authorized Affiliate Claim**"): (i) Customer must bring such Authorized Affiliate Claim directly against Snowflake on behalf of such Authorized

Affiliate, unless Data Protection Laws require the Authorized Affiliate be a party to such claim; and (ii) all Authorized Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set forth in the Agreement, including any aggregate limitation of liability.

3.4 **Customer Processing of Personal Data**. Customer agrees that it: (i) will comply with its obligations under Data Protection Laws with respect to its Processing of Customer Personal Data; (ii) will make appropriate use of the Services to ensure a level of security appropriate to the particular content of the Customer Personal Data, such as pseudonymizing or backing-up Customer Personal Data; and (iii) has obtained all consents, permissions and rights necessary under Data Protection Laws for Snowflake to lawfully Process Customer Personal Data for the Purposes, including, without limitation, Customer's sharing and/or receiving of Customer Personal Data with third-parties via the Services.

3.5 **Details of Data Processing.**

(a) Subject matter: The subject matter of the Processing under this DPA is the Customer Personal Data.

(b) Duration: Notwithstanding expiry or termination of the Agreement, this DPA and Standard Contractual Clauses (if applicable) will remain in effect until, and will automatically expire upon, deletion of all Customer Personal Data as described in this DPA.

(c) Purpose: Snowflake shall Process Customer Personal Data only for the Purposes.

(d) Nature of the Processing: Snowflake provides Services as described in the Agreement.

(e) Categories of Data Subjects: The categories of Data Subjects to which Customer Personal Data relate are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Prospects, customers, business partners and vendors of Customer (who are natural persons);

(ii) Employees or contact persons of Customer's prospects, customers, business partners and vendors; and/or

(iii) Employees, agents, advisors, freelancers of Customer (who are natural persons).

(f) Types of Personal Data: The types of Customer Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Identification and contact data (name, address, title, contact details);

(ii) Financial information (credit card details, account details, payment information);

(iii) Employment details (employer, job title, geographic location, area of responsibility); and/or

(iv) IT information (IP addresses, usage data, cookies data, location data).

(g) Special Categories of Personal Data (if applicable): Subject to any applicable restrictions and/or conditions in the Agreement or Documentation, Customer may also include 'special categories of personal data' (as defined in the GDPR) in Customer Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Customer Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. Sub-processing.

4.1 **Authorized Sub-processors**. Customer specifically authorizes the engagement of those Sub-processors listed at https://www.snowflake.com/legal/snowflake-sub-processors/ ("**Sub-processor Site**") as of the Effective Date and members of the Snowflake Group.

4.2 **Sub-processor Obligations**. Snowflake shall: (i) enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Customer Personal Data as Snowflake's obligations in this DPA to the extent applicable to the nature of the services provided by such Sub-processor; and (ii) remain liable for each Sub-processor's compliance with the obligations in this DPA.

4.3 **Changes to Sub-processors.** Snowflake shall make available on its Sub-processor Site a mechanism for Customer to subscribe to notifications of new Sub-processors. Snowflake shall provide such notification at least fourteen (14) days in advance of allowing the new Sub-processor to Process Customer Personal Data (the "**Objection Period**"). During the Objection Period, Customer may object in writing to Snowflake's appointment of the new Sub-processor, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss Customer's concerns in good faith with a view to achieving resolution. If Customer can reasonably demonstrate that the new Sub-processor is unable to Process Customer Personal Data in compliance with the terms of this DPA and Snowflake cannot provide an alternative Sub-processor, or the parties are not otherwise able to achieve resolution as provided in the preceding sentence, Customer, as its sole and exclusive remedy, may terminate the Order Form(s) with respect only to those aspects of the Services which cannot be provided by Snowflake without the use of the new Sub-processor by providing written notice to Snowflake. Snowflake will refund Customer any prepaid unused fees of such Order Form(s) following the effective date of termination with respect to such terminated Services.

5. Security.

5.1 **Security Measures**. Snowflake shall implement and maintain appropriate technical and organizational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data in accordance with Snowflake's Security Policy found at https://www.snowflake.com/legal ("**Security Policy**"). Customer is responsible for reviewing the information made available by Snowflake relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Snowflake may review and update its Security Policy from time to time, provided that any such updates shall not materially diminish the overall security of the Services or Customer Personal Data.

5.2 **Confidentiality of Processing**. Snowflake shall ensure that any person who is authorized by Snowflake to Process Customer Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.3 **No Assessment of Customer Personal Data by Snowflake**. Customer acknowledges that Snowflake will not assess the contents of Customer Personal Data to identify information subject to any specific legal requirements.

6. Customer Audit Rights.

6.1 Upon written request and at no additional cost to Customer, Snowflake shall provide Customer, or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing Snowflake's compliance with its obligations under this DPA in the form of (i) Snowflake's ISO 27001 and PCI-DSS third-party certifications, (ii) Snowflake's SOC 1 Type II audit reports, SOC 2 Type II audit reports, HIPAA Compliance Report for Business Associates, and (iii) Snowflake's most recently completed industry standard security questionnaire, such as a SIG or CAIQ (collectively, "**Reports**").

6.2 Customer may also send a written request for an audit (including inspection) of Snowflake's facilities. Following receipt by Snowflake of such request, Snowflake and Customer shall mutually agree in advance on the details of the audit, including reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any such audit. Snowflake may charge a fee (rates shall be reasonable, taking into account the resources expended by Snowflake) for any such audit. The Reports, audit, and any information arising therefrom shall be Snowflake's Confidential Information.

6.3 Where the Auditor is a third-party, the Auditor may be required to execute a separate confidentiality agreement with Snowflake prior to any review of Reports or an audit of Snowflake, and Snowflake may object in writing to such Auditor, if in Snowflake's reasonable opinion, the Auditor is not suitably qualified or is a direct competitor of Snowflake. Any such objection by Snowflake will require Customer to either appoint another Auditor or conduct the audit itself. Expenses incurred by Auditor in connection with any review of Reports or an audit, shall be borne exclusively by the Auditor.

7. Data Transfers

7.1 **Hosting and Processing Locations.** Snowflake will only host Customer Personal Data in the region(s) offered by Snowflake and selected by Customer on an Order Form or as Customer otherwise configures via the Services (the "**Hosting Region**"). Customer is solely responsible for the regions from which its Users access the Customer Personal Data, for any transfer or sharing of Customer Personal Data by Customer or its Users and for any subsequent designation of other Hosting Regions (either for the same Account, a different Account, or a separate Service). Once Customer has selected a Hosting Region, Snowflake will not Process Customer Personal Data from outside the Hosting Region except as reasonably necessary to provide the Services procured by Customer, or as necessary to comply with the law or binding order of a governmental body.

7.2 **Transfer Mechanisms.** For any transfers by Customer of Customer Personal Data from the European Economic Area and/or its member states, United Kingdom and/or Switzerland (collectively, "**Restricted Countries**") to Snowflake in a country which does not ensure an adequate level of protection (within the meaning of and to the extent governed by the Data Protection Laws of the Restricted Countries) (collectively, "**Third Country**"), such transfers shall be governed by a valid mechanism for the lawful transfer of Customer Personal Data recognized under Data Protection Laws, such as those directly below:

7.2.1 **For transfers to Snowflake Inc:** Snowflake Inc. shall remain certified under the Privacy Shield and shall comply with the Privacy Shield Principles. If for any reason Snowflake Inc. ceases to be certified under the Privacy Shield or it determines it can no longer meet its obligations to provide the same level of protection as required by the Privacy Shield Principles, Snowflake shall promptly notify Customer and shall work with Customer to take reasonable and appropriate steps to remediate.

7.2.2 **For transfers not covered by 7.2.1 above:** To the extent the transfer mechanism identified in Section 7.2.1 does not apply to the transfer, is invalidated and/or Snowflake Inc. is not self-certified to the Privacy Shield, and Snowflake is located in a Third Country, Snowflake agrees to abide by, and Process Customer Personal Data from the Restricted Countries in compliance with the Standard Contractual Clauses, and for these purposes Snowflake shall be the "data importer" and Customer is the "data exporter" under the Standard Contractual Clauses (notwithstanding that Customer may be an entity located outside of a Restricted Country).

7.2.3 Notwithstanding the foregoing, if Snowflake has adopted Binding Corporate Rules (BCRs) for Processors that cover the transfer of Customer Personal Data to a Third Country, then such BCRs shall govern the transfer of Customer Personal Data.

8. Return or Deletion of Data. Customer may retrieve or delete all Customer Personal Data upon expiration or termination of the Agreement as set forth in the Agreement. Any Customer Personal Data not deleted by Customer shall be deleted by Snowflake promptly upon the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "retrieval period" set forth in the Agreement. Notwithstanding the foregoing, Snowflake shall not be required

to delete Customer Personal Data to the extent Snowflake is required by applicable law or order of a governmental or regulatory body to retain some or all of the Customer Personal Data. Where Snowflake is required to retain Customer Personal Data as set forth in the preceding sentence, then Snowflake will notify Customer of such requirement, to the extent legally permitted.

9. Security Incident Response.

9.1 **Security Incident Reporting.** If Snowflake becomes aware of a Security Incident, Snowflake shall notify Customer without undue delay, and in any case, where feasible, notify Customer within seventy-two (72) hours after becoming aware. Snowflake shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

9.2 **Security Incident Communications.** Snowflake shall provide Customer timely information about the Security Incident, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Snowflake to mitigate or contain the Security Incident, the status of Snowflake's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because Snowflake personnel do not have visibility to the content of Customer Personal Data, it will be unlikely that Snowflake can provide information as to the particular nature of the Customer Personal Data, or where applicable, the identities, number or categories of affected Data Subjects. Communications by or on behalf of Snowflake with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Snowflake of any fault or liability with respect to the Security Incident.

10. Cooperation.

10.1 **Data Subject Requests.** To the extent legally permitted, Snowflake shall promptly notify Customer if Snowflake receives a request from a Data Subject that identifies Customer and seeks to exercise the Data Subject's right to access, rectify, erase, transfer or port Customer Personal Data, or to restrict the Processing of Customer Personal Data ("**Data Subject Request**"). The Service provides Customer with a number of controls that Customer may use to assist it in responding to a Data Subject Request and Customer will be responsible for responding to any such Data Subject Request. To the extent that Customer is unable to access the relevant Customer Personal Data within the Services using such controls or otherwise, taking into account the nature of the Processing, Snowflake shall (upon Customer's written request) provide commercially reasonable cooperation to assist Customer in responding to any Data Subject Requests.

10.2 **Data Protection Impact Assessments.** Snowflake shall provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws, so long as Customer does not otherwise have access to the relevant information.

10.3 **Government Inquiries.** If compelled to disclose Customer Personal Data to a law enforcement or governmental entity, then Snowflake will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Snowflake is legally permitted to do so.

11. Relationship with the Agreement.

11.1 The parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment or exhibit (including the Standard Contractual Clauses (as applicable)) that Snowflake and Customer may have previously entered into in connection with the Services.

11.2 Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Data. Notwithstanding the foregoing, and solely to the extent applicable to any Customer Personal Data comprised of patient, medical or other protected health information regulated by HIPAA or any similar U.S. federal or state health care laws, rules or regulations ("**HIPAA Data**"), if there is any conflict between this DPA and a Business

Associates Agreement between Customer and Snowflake ("**BAA**"), then the BAA shall prevail solely with respect to such HIPAA Data.

11.3 Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPA and any other data protection agreements in connection with the Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Agreement. Without limiting either of the parties' obligations under the Agreement, each party agrees that any regulatory penalties incurred by the one party (the "**Incurring Party**") in relation to the Customer Personal Data that arise as a result of, or in connection with, the other party's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the Incurring Party's liability under the Agreement as if it were liability to the other party under the Agreement.

11.4 In no event shall this DPA or any party restrict or limit the rights of any Data Subject or of any competent supervisory authority.

11.5 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.

Annex A

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

THE PARTIES HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1. Definitions

For the purposes of the Clauses:

'personal data', '**special categories of data**', '**process/processing**', '**controller**', '**processor**', '**data subject**' and '**supervisory authority**' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

'the data exporter' means the controller who transfers the personal data;

'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Subprocessing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data

importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

11.2 The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data processing services

12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Data exporter*:* The data exporter is the entity identified as the "Customer" in the Data Processing Addendum in place between data exporter and data importer and to which these Clauses are appended ("**DPA**").

Data importer*:* The data importer is **Snowflake** (as defined in the DPA) to the extent based in a Third Country (as defined in the DPA and described in Section 7.2.2). Snowflake provides enterprise cloud computing solutions, which process Customer Personal Data upon the instruction of the Customer in accordance with the terms of the Agreement.

Description of Data Processing: Please see Section 3.5 (Details of Processing) of the DPA for a description of the categories of data subjects, categories of data, special categories of data and processing operations.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see the Security Policy at https://www.snowflake.com/legal, which describes the technical and organisational security measures implemented by Snowflake.

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Clause 5(a): Suspension of data transfers and termination:

1. If the data exporter intends to suspend the transfer of personal data and/or terminate the Standard Contractual Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").

2. If after the Cure Period the data importer has not or cannot cure the non-compliance, then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 6 (Customer Audit Rights) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to any aggregate limitations on liability set out in the Agreement. In no event shall any party limit its liability to a data subject with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that Article 28 of the GDPR allows for the general written authorisation of a subprocessor subject to notice of, and the opportunity to object to, the subprocessor. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of the Standard Contractual Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 4 (Sub-processing) of the DPA.