Data Processing Addendum

This Data Processing Addendum, and all its attachments (this "**DPA**") is incorporated into the Master Subscription Agreement (the "**MSA**") between the undersigned Customer and BetterCloud, Inc. ("**BetterCloud**"). Capitalized but undefined terms used in this DPA will have the meanings assigned to those terms in the MSA.

In the course of providing the Services to Customer pursuant to the MSA, BetterCloud may Process Personal Data on behalf of Customer. BetterCloud agrees to comply with the following provisions with respect to its Processing of Customer Personal Data.

1. DEFINITIONS

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

"**Customer Personal Data**" means Personal Data submitted or provided by or for Customer, or at Customer's direction, to BetterCloud in connection with Customer's use of the Services, and to which Data Protection Laws apply.

"**Data Protection Laws**" means all data privacy laws and regulations, including data privacy laws and regulations of the European Union ("**EU**"), the European Economic Area ("**EEA"**) and their member states, Switzerland, and the United Kingdom ("**UK**"), applicable to the Processing of Customer Personal Data by BetterCloud under the MSA.

"**Data Subject**" means an identified or identifiable natural person about whom BetterCloud Processes Personal Data in connection with the Services.

"**DPA Effective Date**" means the date on which the parties execute this DPA.

"**GDPR**" means the EU General Data Protection Regulation 2016/679.

"**Personal Data**" means any information which relates to an identified or identifiable natural person, and to which Data Protection Laws apply.

"**Personal Data Breach**" means a breach of BetterCloud's security leading to the unauthorized, accidental or unlawful destruction, loss, alteration, disclosure of, or access to, Customer Personal Data in BetterCloud's possession, custody or control.

"**Process/Processing**" shall have the same meaning as in GDPR.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

"**Security Documentation**" means the security measures applicable to the Services purchased by Customer, as described in Annex II of the SCCs and the summaries of the then-current SSAE 16 SOC Type II audit reports (or comparable industry-standard successor report) that BetterCloud generally makes available to its customers as updated from time to time, or otherwise made reasonably available by BetterCloud.

"**Standard Contractual Clauses**" or "**SCCs**" means the agreement executed by and between Customer and BetterCloud and attached to this Addendum as Attachment 2 in accordance with the European Commission Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"**Sub-processor**" means any entity that BetterCloud engages to Process Customer's Personal Data on behalf of BetterCloud as part of the Services.

"Transparency Report" is the publicly available report including information regarding requests made by government agencies or law enforcement officials to obtain Personal Data from BetterCloud and that is located at https://www.bettercloud.com/transparencyreport/ or at such other URL as BetterCloud may provide from time to time.

2. PROCESSING OF CUSTOMER PERSONAL DATA

2.1 **Roles of the Parties**; **Purpose**. The parties acknowledge and agree that with regard to the Processing of Customer Personal Data, Customer is the Controller, BetterCloud is a Processor and that BetterCloud may engage Sub-processors pursuant to the requirements set forth herein.

2.2 **BetterCloud's Processing of Personal Data**. BetterCloud shall only Process Customer Personal Data on behalf of and in accordance with Customer's instructions. Customer instructs BetterCloud to Process Customer Personal Data for the following purposes: (i) Processing in accordance with the MSA, the DPA and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the MSA and this DPA. This DPA and the MSA are Customer's complete and final instructions to BetterCloud for the Processing of Customer Personal Data. Any additional or alternate instructions must be agreed upon separately in writing signed by authorized representatives of both parties.

2.3 **Customer's Processing of Personal Data**. Customer shall, in its use of the Services, Process Customer Personal Data in accordance with the requirements of Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Personal Data.

2.4 **Security of Processing**. BetterCloud will secure Customer Personal Data by implementing appropriate technical and organizational measures designed to provide a level of security appropriate to the risk, as required under the applicable Data Protection Laws. Such measures include those set forth in the Security

Documentation. BetterCloud will not materially decrease the overall security of the Services during the term of the MSA.

2.5 **BetterCloud's Security Assistance**. BetterCloud will (taking into account the nature of the processing of Customer Personal Data and the information available to BetterCloud) provide Customer with reasonable assistance necessary for Customer to comply with its obligations in respect of Customer Personal Data under Data Protection Laws, including Articles 32 to 34 (inclusive) of the GDPR, by (a) implementing the security measures in accordance with Section 2.4 (Security of Processing); (b) complying with the terms of Section 2.8 (Personal Data Breach Notification); and (c) providing Customer with the third-party certifications and summaries of the audit reports set forth in the Security Documentation in accordance with Section 2.14 (Audits).

2.6 **Customer's Security Responsibilities**. Customer agrees that, without prejudice to BetterCloud's obligations under Section 2.8 (Personal Data Breach Notification), Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; and (c) backing up its Customer Personal Data.

2.7 **Customer's Security Assessment**. Customer is solely responsible for reviewing the Security Documentation and the security measures listed in Annex II of the SCCs, if applicable, and evaluating for itself whether the Services, the Security Documentation and BetterCloud's data security commitments under this DPA and the SCCs, if applicable, will meet Customer's needs, including with respect to any security obligations of Customer under the Data Protection Laws.

2.8 **Personal Data Breach Notification**. BetterCloud will notify Customer without undue delay after becoming aware of a Personal Data Breach. BetterCloud shall make reasonable efforts to identify and remediate the cause of such Personal Data Breach and will provide sufficient information to Customer to allow Customer to meet any obligations to report or inform individuals or regulators of the Personal Data Breach. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Personal Data Breach. BetterCloud's notification of or response to a Personal Data Breach under this Section 2.8 will not be construed as an acknowledgement by BetterCloud of any fault or liability with respect to the Personal Data Breach.

2.9 **Impact Assessments and Consultations**. BetterCloud will (taking into account the nature of the processing and the information available to BetterCloud) reasonably assist Customer in complying with its obligations under Data Protection Laws in respect of data protection impact assessments and prior consultation, including, if applicable, Customer's obligations pursuant to Articles 35 and 36 of the GDPR.

2.10 **Data Subject Rights.** During the term of the MSA, if BetterCloud receives any request from a Data Subject in relation to Customer Personal Data, BetterCloud will promptly notify Customer of such request and Customer will be responsible for responding to any such request unless otherwise authorized by the Customer or required by Data Protection Laws. Upon request from Customer, BetterCloud shall provide

commercially reasonable assistance to Customer in relation to the handling of a Data Subject's request for exercising the Data Subject's rights laid down in the Data Protection Laws, taking into account the nature of BetterCloud's Processing of Customer Personal Data and solely to the extent Customer is unable to fulfill such requests through the Services. Customer shall be responsible for any costs arising from BetterCloud's provision of such assistance.

2.11 **Deletion of Customer Personal Data**. BetterCloud shall delete all Customer Personal Data and copies thereof upon request of Customer, unless otherwise required by the applicable Data Protection Laws, provided, however, that BetterCloud shall delete backup data and operational or system log data in the ordinary course of business. In the event applicable law does not permit BetterCloud to delete the Customer Personal Data, BetterCloud warrants that it shall ensure the confidentiality of the Customer Personal Data and that it shall not use or disclose any Customer Personal Data after termination of the MSA, except as required by law.

2.12 **Data Storage and Processing Facilities**. BetterCloud may, subject to Section 2.13 (Data Transfers), store and process Customer Personal Data anywhere BetterCloud or its Sub-processors maintain facilities.

2.13 **Data Transfers.** With respect to Customer Personal Data transferred from the EEA to outside the EEA, from the UK to outside of the UK, or from Switzerland to outside of Switzerland in conjunction with Customer's use of the Services, either directly or via onward transfer, the SCCs will apply, subject to the provisions of Attachment 1.

2.14 **Audits**.

(a) BetterCloud will make available to Customer all information reasonably necessary to demonstrate compliance with its obligations under the Data Protection Laws. Upon Customer's written request at reasonable intervals, BetterCloud shall provide a copy of BetterCloud's then most recent summaries of third-party audits or certifications, as applicable, that BetterCloud generally makes available to its customers at the time of such request.

(b) If Customer reasonably believes it needs further information in order to confirm BetterCloud's compliance with the provisions of this DPA relating to Customer Personal Data, BetterCloud will use commercially reasonable efforts to respond to written questions by Customer regarding the Security Documentation.

(c) If Customer is not satisfied with BetterCloud's responses to questions provided pursuant to Section 2.14.(b) and if GDPR or the SCCs grant Customer the right to audit BetterCloud's Processing activities covered under this DPA, then BetterCloud shall permit Customer to audit BetterCloud's compliance with the data security and data protection obligations under this DPA. Customer may request such audit no more than once in each twelve (12) month period and it shall be conducted during BetterCloud's regular business hours. In order to request an audit, Customer shall (1) notify BetterCloud in writing via email to privacy@bettercloud.com at least thirty (30) days in advance, detailing the dates and duration of the audit and the identity and the qualifications of the auditor, (2) agree in writing with BetterCloud on (i) the scope of the audit, (ii) the security and confidentiality controls required for access to the information, facilities or processes in scope of such audit, and (iii) the reasonable reimbursement rate for which Customer shall be responsible, and (3) cause such auditor to sign a non-disclosure agreement that is satisfactory to BetterCloud with BetterCloud. BetterCloud may object to any external auditor if, in BetterCloud's reasonable

opinion, the auditor is not qualified, does not have an appropriate security clearance, is a competitor to BetterCloud, or is not independent. If BetterCloud objects to the identity or qualifications of any proposed auditor, BetterCloud shall provide, in writing, a reason for such objection and Customer will be required to propose another auditor. All information provided or made available to Customer or its auditor pursuant to such audit shall be considered BetterCloud's Confidential Information.

(d) The parties agree that the audit rights described in Article 28 of the GDPR shall be satisfied by this Section 2.14.

2.15 **Processing Records**. Customer acknowledges that BetterCloud is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which BetterCloud is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer Personal Data, Customer will, where requested, provide such information to BetterCloud, and will ensure that all information provided is kept accurate and up-to-date.

3. SUB-PROCESSORS

3.1 **General Authorization**. Customer authorizes and consents to BetterCloud engaging Sub-processors to process Customer Personal Data under this DPA. BetterCloud will: (a) provide Customer with such details about the Sub-processor(s) it uses as may be reasonably requested by Customer from time to time; (b) flow down its obligations under this DPA to such Sub-processor, such that the data processing requirements of such Sub-processor with respect to Customer Personal Data are no less onerous than the data processing requirements of BetterCloud as set out in this DPA; and (c) be fully liable to Customer for the performance of the Sub-processor's obligations under this DPA if such Sub-processor fails to fulfill its data protection obligations. Information about the Sub-processors that BetterCloud uses, including their functions and contact details, is available at https://www.bettercloud.com/subprocessors (as may be updated by BetterCloud from time to time in accordance with this DPA).

3.2 **New Sub-Processors**. BetterCloud will inform Customer of any intended changes concerning the addition or replacement of Sub-processors at least ten (10) days prior to permitting any new Sub-processor to process Personal Data if Customer subscribes to notifications of updates to the list of Sub-processors by using the mechanism set forth at https://www.bettercloud.com/subprocessors. If Customer has a reasonable basis to object to BetterCloud's use of a new Sub-processor, Customer shall notify BetterCloud promptly in writing within ten (10) days after BetterCloud informs Customer of such change. If such objection is not unreasonable, BetterCloud will use reasonable efforts to make available to Customer a change in the affected Services or recommend a commercially reasonable change to Customer's configuration or use of the affected Services to avoid processing of Customer Personal Data by such new Sub-processor. If BetterCloud is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Order Form(s) in respect only to those Services which cannot be provided by BetterCloud without the use of the objected-to new Sub-processor, by providing written notice to BetterCloud. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services.

4. **GENERAL PROVISIONS**.

4.1 **Conflicting Terms**. This DPA applies only between Customer and BetterCloud and does not confer any rights to any third party. To the extent of any conflict or inconsistency between this DPA and the MSA, this DPA will govern. This DPA replaces and supersedes all prior and contemporaneous agreements concerning its subject matter.

4.2 **Term and Termination**. This DPA will become effective as of the DPA Effective Date. This DPA will terminate simultaneously and automatically upon the termination of the MSA, or when BetterCloud ceases Processing Customer Personal Data, whichever is later.

4.3 **Liability**. The total liability of either party and its Affiliates towards the other party and its Affiliates, whether in contract, tort or any other theory of liability, under or in connection with this DPA will be limited to limitations on liability or other liability caps agreed to by the parties in the MSA.

4.4 **Governing Law**. This DPA shall be governed by the laws and the jurisdiction stated in the MSA.

IN WITNESS WHEREOF, this Data Processing Addendum has been executed by duly authorized signatories of Customer and BetterCloud as of the later date set forth below.

ACCEPTED AND AGREED TO;

CUSTOMER:	BETTERCLOUD, INC.
By: _____ Authorized Signature	By: _____ Authorized Signature
Print Name: _____	Print Name: R. Bart Hacking
Title: _____	Title: Chief Financial Officer
Date: _____	Date: _____
Email address for notifications to Customer under this DPA: _____	Internal Use: _____

Attachment 1
Additional Data Transfer Terms

Additional terms to the Standard Contractual Clauses applicable pursuant to Section 2.13 of the DPA for Customer Personal Data transferred from the EEA to outside the EEA, from the UK to outside of the UK, or from Switzerland to outside of Switzerland in conjunction with Customer's use of the Services, either directly or via onward transfer:

1. **Instructions.** For purposes of Clause 8.1 of the SCCs, the parties agree that Section 2.2. of the DPA and Annex I of the SCCs contain the instructions of Customer for BetterCloud's processing of Customer Personal Data.

2. **Certification of deletion.** Customer agrees that the certification of deletion of Personal Data that is described in Clause 8.5 of the SCCs shall be provided by BetterCloud to Customer only upon Customer's written request.

3. **Personal Data Breaches.** The parties agree that if a Sub-processor suffers a personal data breach affecting Customer Personal Data, BetterCloud will take commercially reasonable efforts to ensure that the Sub-processor takes appropriate measures to address the breach, including measures to mitigate its adverse effects in accordance with Clause 8.6.(c) of the SCCs.

4. **Audits and certifications.** Customer agrees that Section 2.14 of the DPA satisfies Customer's rights under Clauses 8.9.(c) and 8.9.(d) of the SCCs.

5. **Notification of new Subprocessors.** Customer consents to BetterCloud's transfer of Customer Personal Data to Sub-processors as described in Sections 3.1 and 3.2 of the DPA, and agrees that this Customer's consent satisfies the requirements of Clauses 9(a) and 9(b) of the SCCs.

6. **BetterCloud's obligations in case of access by public authorities**. BetterCloud will frequently update the Transparency Report. To the extent permitted by applicable laws, BetterCloud will inform Customer of any request it receives to disclose Personal Data if Customer subscribes to receive such notifications by using the mechanism set forth at https://www.bettercloud.com/transparencyreport/. Customer agrees that the mechanism described herein satisfies the requirements under Clause 15.1(c) of the SCCs.

7. **Conflict.** In the event of any conflict or inconsistency between (i) the body of this DPA, (ii) this Attachment 1, and (iii) the SCCs in Attachment 2, the order of precedence shall be: (i) the SCCs in Attachment 2, (ii) Attachment 1, and (iii) the body of this DPA.

Attachment 2

Standard Contractual Clauses

MODULE TWO: CONTROLLER TO PROCESSOR

SECTION I

Clause 1

Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

b. The Parties:
   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, Standard Contractual Clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

This does not prevent the Parties from including the Standard Contractual Clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   ii. Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);
   iii. Clause 9 - Clause 9(a), (c), (d) and (e);
   iv. Clause 12 - Clause 12(a), (d) and (f);
   v. Clause 13;
   vi. Clause 15.1(c), (d) and (e);
   vii. Clause 16(e);
   viii. Clause 18 - Clause 18(a) and (b).

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional
Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content

or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

a. GENERAL WRITTEN AUTHORISATION. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfill its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
   i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
   ii. refer the dispute to the competent courts within the meaning of Clause 18.

d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

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

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   ii. the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;[4]
   iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that are not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right of termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable

procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   ii. the data importer is in substantial or persistent breach of these Clauses; or
   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18
Choice of forum and jurisdiction

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b. The Parties agree that those shall be the courts of the Republic of Ireland.

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name:
Address:
Contact person's:
Name:
Position:
Contact details:
Activities relevant to the data transferred under these Clauses: As set forth in the MSA and the DPA.

Signature: _____
Date: _____
Role (controller/processor): Controller

Data importer(s):

1. Name: BetterCloud, Inc.
Address: 330 7th Avenue 4th Floor, New York, NY 10001, USA
Contact person's:
Name: Legal Department
Position: Legal Department
Contact details: privacy@bettercloud.com
Activities relevant to the data transferred under these Clauses: As set forth in the MSA and the DPA.

Signature: _____
Date: _____
Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Data exporter may submit or provide Customer Personal Data to data importer, the extent of which is determined and controlled by data exporter in its sole discretion and which may include, but is not limited to, Customer Personal Data relating to the following categories of data subjects:

- Employees of the data exporter and any affiliate entities.
- Independent contractors of the data exporter and any affiliate entities.

Categories of personal data transferred
Data exporter may submit or provide Customer Personal Data to data importer, the extent of which is determined and controlled by data exporter in its sole discretion, and which may include, but is not limited to the following categories of Customer Personal Data:

- Name, Email, Phone, Photo, Title, Address, Department, Manager, IP address, user activity, helpdesk tickets, satisfaction data.
- Payment information.
- Other Customer Personal Data the data exporter submits or provides to the data importer in the course of using the Services including through its use of the content scanning features included in the Services.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
Data importer does not require special categories of data to provide the Services, but it may process such special categories of data if submitted or provided to data importer by the data exporter including through its use of the content scanning features included in the Services.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Continuous for the duration of the provision of the Services.

Nature of the processing
BetterCloud's provision of the Services to Customer.

Purpose(s) of the data transfer and further processing

BetterCloud will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with the Agreement, the DPA and any additional instruction agreed to in writing by the parties.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
Customer Personal Data will be retained as agreed by the parties in the Agreement and the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
The subject matter, nature and duration of the processing is set forth in the MSA and the DPA. See https://www.bettercloud.com/subprocessors/ for additional information.

C. COMPETENT SUPERVISORY AUTHORITY

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

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measures of encryption of personal data; Measures for the protection of data during storage; Measures for the protection of data during transmission

- BetterCloud uses Industry Standard[5] encryption to secure Customer Personal Data in transit outside of BetterCloud Systems[6] and at rest in all locations where it is stored.
- BetterCloud uses TLS 1.2. or higher when transferring Customer Personal Data over the internet.
- BetterCloud uses encryption-at-rest, which protects data with AES-256 or AES-128 encryption.
- Full disk or device encryption is required for all systems that store Customer Personal Data.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- BetterCloud implements Industry Standard firewalls which manage and restrict network traffic and properly segment its network and systems storing Customer Personal Data.
- BetterCloud uses an Industry Standard intrusion detection system to detect inappropriate, incorrect, or anomalous activity, and BetterCloud regularly monitors system logs for suspicious activity.
- BetterCloud establishes and follows commercially reasonable operational procedures to stop or mitigate any real or reasonably foreseeable potential attack or attempted attack.
- BetterCloud maintains vulnerability and patch management processes and tools which regularly assess software for security vulnerabilities and deploys software patches and updates.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- BetterCloud performs daily backups of all systems and data.
- BetterCloud maintains copies of backups in a location separate from the primary data location.
- BetterCloud performs disaster recovery and service restoration testing on at least an annual basis to ensure that restoration can be performed in a timely manner.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- BetterCloud monitors the effectiveness of its security program by conducting self-audits and risk assessments of the BetterCloud Systems against the documented policies and guidelines

[5] "Industry Standard" means then-current industry standard practices relating to information and infrastructure security and privacy, provided that such standards shall be consistent with SOC 2, ISO/IEC 27001, or the CSA CCM (and all applicable successor provisions).

[6] "BetterCloud Systems" means BetterCloud's networks, platforms, devices, systems, servers, workstations, services, technology, and applications that Process Customer Personal Data.

maintained by BetterCloud, including penetration and vulnerability tests conducted by a reputable third party, on at least an annual basis.

- BetterCloud uses external auditors to verify the adequacy of its security measures. Such audits: (a) are performed according to AICPA SOC 2 standards for security and confidentiality or such other alternative standards that are substantially equivalent to AICPA SOC 2; (b) are performed by independent third-party security professionals; and (c) result in the generation of an audit report.
- BetterCloud maintains certification of its information security management system based on the ISO/IEC 27001 criteria.

Measures for user identification and authorisation

- BetterCloud personnel accessing Customer Personal Data are identified by a unique user ID.
- Access to the BetterCloud Systems and Customer Personal Data located thereon requires a user ID and password.
- Passwords for access to Customer Personal Data are stored securely using Industry Standard. encryption, not in plain text, on a separate server or file from Customer Personal Data.

Measures for ensuring physical security of locations at which personal data are processed

- BetterCloud maintains Industry Standard physical security controls and procedures over all BetterCloud facilities where Customer Personal Data is Processed, including (at a minimum): appropriate alarm systems; access controls (including off-hours controls); visitor access procedures; fire suppression; environmental controls.
  (in each case to the extent that such security perimeters are within BetterCloud's control.)
- Passage through the physical barriers at BetterCloud facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., receptionist, etc.).
- Visitors are required to sign-in.
- BetterCloud securely stores physical files, workstations, and devices that contain Customer Personal Data.
- BetterCloud maintains safety standards in place when Customer Personal Data is en route, including:
  - training of BetterCloud personnel regarding safe security practices; and
  - technical controls such as encryption of laptops, thumb drives, files, and disks to prevent access to Customer Personal Data if the physical device or media is lost.

Measures for ensuring events logging

- BetterCloud logs all application, system, and cloud console events to centralized log repositories that provide automated inspection of the logs for security issues and anomalous activity. Alerts are generated and sent to information security staff for investigation and resolution.

Measures for ensuring system configuration, including default configuration; Measures for certification/assurance of processes and products

- BetterCloud utilizes an infrastructure as code system to control the configuration and deployment of all production systems. Any changes made to systems outside of the infrastructure as code processes are alerted on and automatically reverted to comply with configuration standards.

Measures for internal IT and IT security governance and management; Measures for ensuring accountability

- BetterCloud maintains a compliance team dedicated to provide governance and ensure compliance with BetterCloud's IT and IT security policies.
- To provide assurance of the governance process, BetterCloud's policies and procedures are externally audited annually and cataloged in BetterCloud's SOC2 Type II report.

Measures for assisting the data exporter with data subject requests

- If BetterCloud receives a data subject request, BetterCloud will promptly notify the data exporter of such data subject request.
- If the data exporter requests BetterCloud's assistance in handling the data subject request, BetterCloud shall provide commercially reasonable assistance to the data exporter in accordance with Section 2.10 of the DPA.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:

BetterCloud's third-party security management program ensures all Sub-processors meet BetterCloud's security and privacy standards. Every Sub-processor shall:

- Have a data processing agreement including the appropriate Standard Contractual Clauses or other valid data transfer mechanism in compliance with GDPR.
- Verify the adequacy of its security measures according to AICPA SOC 2 standards or maintain a certification of its information security management system based on the IS027001 criteria.
- Perform penetration tests conducted by a reputable third party.
- Use encryption to secure Customer Personal Data in transit and at rest.
- Have a risk management plan.
- Have a disaster recovery plan.
- Have a vulnerability management plan.

ANNEX III – LIST OF SUB-PROCESSORS

See https://www.bettercloud.com/subprocessors/ for the name, contact details, and description of processing of BetterCloud's Sub-processors.