Cloudwick 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 Cloudwick and Customer for Customer's purchase of Services from Cloudwick that references this DPA (the "Agreement"). By signing the Agreement, the parties enter into this DPA on behalf of themselves and, to the extent required under applicable Data Protection Laws, in the name and on behalf of their Affiliates authorized to provide or receive (as applicable) the Services, and this DPA shall be effective on the effective date of the Agreement ("Effective Date").

If the parties entered into a data processing addendum or other similar agreement before November 2017 (any "Prior DPA"), the parties acknowledge and agree that this DPA shall supersede and replace the Prior DPA as of the Effective Date. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

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

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

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

"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.

"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.

"EU Data Protection Law" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of

Personal Data and on the free movement of such data ("Directive") and (ii) on and after 25 May 2018, 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"), and repealing Directive 95/46/EC.

"EEA" means, for the purposes of this DPA, the European Economic Area and/or its member states, United Kingdom and/or Switzerland.

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

"Personal Data" means any information relating to an identified or identifiable natural person.

"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" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

"Purposes" shall mean the data processing purposes described and defined in Section 3.4 of this DPA.

"Security Incident" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data, but does not include any Unsuccessful Security Incident.

"Services" means the Service provided by Cloudwick to Customer pursuant to the Agreement and any Support Services and Technical Services (formerly referred to as Professional Services) provided by Cloudwick to Customer pursuant to the Agreement.

"Sensitive Personal Data" means any 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.

"Sub-processor" means any Data Processor engaged by Cloudwick or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or Cloudwick's Affiliates.

"Unsuccessful Security Incident" means an unsuccessful attempt or activity that does not compromise the security of Customer Personal Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts,

denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

2. Scope and Applicability of This DPA

2.1 This DPA applies where and only to the extent that Cloudwick Processes Customer Personal Data on behalf of Customer as Data Processor in the course of providing Services pursuant to the Agreement.

2.2 Part B shall only apply to Customer Personal Data within the scope of the DPA that is subject to applicable Data Protection Laws of the EEA and shall apply in addition to and not in substitution for, the terms in Part A and Part C.

2.3 Notwithstanding expiry or termination of the Agreement, this DPA and Model Clauses (if applicable) will remain in effect until, and will automatically expire upon, deletion of all Customer Personal Data by Cloudwick as described in this DPA.

PART A: GENERAL DATA PROTECTION OBLIGATIONS

3. Roles and Scope of Processing

3.1 Role of the Parties. As between Cloudwick and Customer, Customer is either the Data Controller of Customer Personal Data, or in the case that Customer is acting on behalf of a third-party Data Controller, then a Data Processor, and Cloudwick shall process Customer Personal Data only as a Data Processor acting on behalf of Customer. To the extent any Service Data (as defined in the Agreement) is considered Personal Data under Applicable Data Protection Laws, Cloudwick is the Data Controller of such data and shall process such data in accordance with the Agreement and applicable Data Protection Laws. Page 3 of 18 Cloudwick-Customer DPA (GDPR Version) 2018May16 Cloudwick Confidential

3.2 Customer Processing of Personal Data. Customer agrees that: (i) it will comply with its obligations under Data Protection Laws in respect of its processing of Personal Data, including any obligations specific to its role as a Data Controller (where Data Protection Laws recognise such concept); (ii) it has provided all notice and obtained all consents, permissions and rights necessary under Data Protection Laws for Cloudwick to lawfully process Personal Data for the Purposes; and (iii) it 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. If Customer is itself a Data Processor acting on behalf of a third-party Data Controller, Customer warrants to Cloudwick that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Cloudwick as another Data Processor, have been authorized by the relevant Data Controller.

3.3 Customer Instructions. Cloudwick will process Customer Personal Data only for the Purposes and in accordance with Customer's documented lawful instructions. The parties agree that the Agreement (including this DPA) sets out the Customer's complete and final instructions to Cloudwick in relation to the processing of Customer Personal Data. Additional processing outside the scope of these instructions (if any) will require prior written agreement between Customer and Cloudwick.

3.4 Details of Data Processing

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

(b) Duration: As between Cloudwick and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

(b) Duration: As between Cloudwick and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

(c) Purpose: Customer Personal Data may only be processed by Cloudwick solely for the following purposes: (i) the provision of the Services to the Customer as further described in the Agreement and the performance of Cloudwick's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties in mutually executed written form; and (ii) processing initiated by Users in their use of the Services (the "Purposes").

(d) Nature of the processing: Cloudwick provides enterprise cloud computing solutions and such as other Services as described in the Agreement, which process Customer Personal Data upon the instruction of the Customer in accordance with the terms of the Agreement.

(e) Categories of data subjects: Customer may submit Customer Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

(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;

(iii) Employees, agents, advisors, freelancers of Customer (who are natural persons); and/or

(iv) Eustomer's end-users authorized by Customer to use the Services.

(f) Types of Personal Data: Customer may submit Customer Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, the following types of Personal Data:

(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) Sensitive Personal Data (if applicable): Certain Editions of Cloudwick's Service have enhanced technical and organizational security measures, such as Cloudwick's "Enterprise for Sensitive Data Edition" and Cloudwick's "Virtual Private Cloudwick Edition." Customer must determine whether particular Services have appropriate technical and organizational security measures for Sensitive Personal Data. If Customer determines the Services have appropriate measures, then subject to any restrictions and/or conditions in the Agreement or Documentation, Customer may submit Sensitive Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, the following types of Sensitive Personal Data:

(i) Protected health information

(ii) Any other information that is Sensitive Personal Data (as defined under this DPA)

3.5 Access or Use. Cloudwick will not access or use Customer Personal Data, except as necessary for the Purposes, or as necessary to comply with the law or binding order of a governmental body.

4. Subprocessing

4.1 Authorized Sub-processors. Subject to Section 9 (Changes to Sub-Processors), Customer agrees that Cloudwick may engage Sub-processors to process Customer Personal Data on Customer's behalf. The Subprocessors currently engaged by Cloudwick and authorized by Customer are listed in Annex A.

4.2 Sub-processor Obligation. Cloudwick will: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Personal Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Cloudwick to breach any of its obligations under this DPA.

5. Security

5.1 Security Measures. Cloudwick 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 Cloudwick's security standards described in Annex B ("Security Measures").

5.2 Updates to Security Measures. Customer is responsible for reviewing the information made available by Cloudwick 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. Customer acknowledges that the Security Measures are subject to technical progress and development and that Cloudwick may update or modify the Security Measures

from time to time provided that such updates and modifications do not result in a material degradation of the overall security of the Services subscribed to by Customer. Page 5 of 18 Cloudwick-Customer DPA (GDPR Version) 2018May16 Cloudwick Confidential

5.3 Confidentiality of processing. Cloudwick shall ensure that any person who is authorized by Cloudwick 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).

5.4 No Assessment of Customer Data by Cloudwick. Customer acknowledges that Cloudwick will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incidents.

5.5 Customer Responsibilities. Customer agrees that, without prejudice to Cloudwick's obligations under Section 5.1 (Security Measures) and Section 9.3 (Security Incident Response):

(a) Customer is responsible for its use of the Services, including making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data, securing its account authentication credentials, managing its data back-up strategies, and protecting the security of Customer Personal Data when in transit to and from the Services and taking any appropriate steps to pseudonymize, securely encrypt, and/or backup any Customer Personal Data uploaded to the Services;

(b) Cloudwick has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Cloudwick's and its Sub-processors' systems (for example, offline or onpremise storage).

6. Security Reports and Audits

6.1 Customer acknowledges that Cloudwick is regularly audited by independent third-party auditors and/or internal auditors against the standards specified in the Cloudwick Security Policy, as described in Annex B. Upon request, Cloudwick shall supply (on a confidential basis) a summary copy of its then-current audit report(s) ("Report") to Customer, so that Customer can verify Cloudwick's compliance with this DPA. Notwithstanding the foregoing, Customer may disclose a Report as allowed under the applicable confidentiality section of the Agreement, including where requested or required by data protection authorities having jurisdiction over Customer even if not legally required ("Data Protection Authority Request"), provided, however, that Customer shall give Cloudwick prior written notice of the Data Protection Authority Request such that Cloudwick can attempt to secure confidential treatment for the Report. If Customer is not legally permitted to give Cloudwick prior notice, Customer agrees to use reasonable efforts to secure confidential treatment for the Report and further agrees to not remove or obscure any "confidential", "proprietary", or similar markings from the Report.

6.2 Cloudwick shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its Processing of Customer Personal Data, including responses to information security and audit questionnaires that are necessary to confirm Cloudwick's compliance with this DPA, provided that Customer shall not exercise this right more than once per year, except that this right may also be exercised in the event Customer is expressly requested or required to provide this information to a data protection authority, or Cloudwick has experienced a Security Incident, or other reasonably similar basis.

7. International Transfers

7.1 Cloudwick hosts Customer Data in the region selected by Customer (specified in the Agreement, an Order Form, and/or as requested by Customer), provided, however that Cloudwick may process Customer Data anywhere in the world where Cloudwick, its Affiliates or its Sub-processors maintain data processing Cloudwick Confidential operations. Cloudwick will at all times provide appropriate safeguards for the Customer Personal Data wherever it is processed, in accordance with the requirements of Data Protection Laws.

8. Co-operation

8.1 If a law enforcement agency sends Cloudwick a demand for Customer Personal Data (e.g., a subpoena or court order), Cloudwick will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Cloudwick may provide Customer’s contact information to the law enforcement agency. If compelled to disclose Customer Personal Data to a law enforcement agency, then Cloudwick will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Cloudwick is legally permitted to do so.

9. Return or Deletion of Data

9.1 Deletion by Customer. Cloudwick will enable Customer to delete Customer Data during the Subscription Term in a manner consistent with the functionality of the Service.

9.2 Deletion on Termination. For 30 days following termination or expiration of the Agreement, Customer shall have the option to retrieve any remaining Customer Personal Data in accordance with the Agreement. Thereafter, Customer instructs Cloudwick to automatically delete all remaining (if any) Customer Personal Data (including copies). Cloudwick shall not be required to delete Customer Personal Data to the extent (i) Cloudwick is required by applicable law or order of a governmental or regulatory body to retain some or all of the Customer Personal Data; and/or (ii), Customer Personal Data has been archived on back-up systems, which Customer Personal Data Cloudwick shall securely isolate and protect from any further processing, except to the extent required by applicable law.

Part B: EEA Specific Provisions

9.3 Security Incident Response. Upon confirming a Security Incident, Cloudwick shall: (i) notify Customer without undue delay, and in any event such notification shall, where feasible, occur no later than 72 hours from Cloudwick confirming the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) Cloudwick shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Cloudwick's notification of or response to a Security Incident under this Section 9.3 (Security Incident Response) will not be construed as an acknowledgment by Cloudwick of any fault or liability with respect to the Security Incident.

10. Changes to Sub-processors.

10.1 Cloudwick shall (i) provide an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer (for which email will suffice) if it adds or removes Sub-processors at least fourteen (14) days' prior to allowing such Sub-processor to process Customer Personal Data.

10.2 Customer may object in writing to Cloudwick's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If Cloudwick 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 Agreement (including this DPA but shall not be eligible for any refund and Customer must immediately pay all fees payable under the Agreement.

11. Cooperation

11.1 The Services provide Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Personal Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. 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, Cloudwick shall (at Customer's request and expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Customer Personal Data under the Agreement. In the event that any request from individuals or applicable data protection authorities is made directly to Cloudwick where such request identifies Customer, Cloudwick shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so, and instead, after being notified by Cloudwick, Customer shall respond. If Cloudwick is

required to respond to such a request, Cloudwick will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

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

11.3 To the extent Cloudwick is required under EU Data Protection Law, Cloudwick shall (at Customer's request and expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

12. EEA Data Transfers

12.1 Transfer mechanism: To the extent that Cloudwick processes any Customer Personal Data protected by applicable Data Protection Laws of the EEA ("EEA Data"), the parties agree that Cloudwick makes available the transfer mechanisms listed below, for any transfers of EEA Data from the EEA to Cloudwick located in a country which does not ensure an adequate level of protection (within the meaning of applicable Data Protection Law) and to the extent such transfers are subject to such Data Protection Laws of the EEA:

(a) If and when Cloudwick is self-certified to the Privacy Shield: (i) the parties acknowledge and agree that Cloudwick will be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for EEA Data by virtue of having self-certified its compliance with the Privacy Shield; (ii) Cloudwick agrees to process EEA Data in compliance with the Privacy Shield Principles; and (iii) if Cloudwick is unable to comply its obligations under this sub-Section, Cloudwick will inform the Customer.

(b) To the extent the transfer mechanism identified in Section 13.1(a) does not apply to the transfer, is invalidated and/or Cloudwick is not self-certified to the Privacy Shield, Cloudwick agrees to abide by and process EEA Data in compliance with the Model Clauses and for these purposes Cloudwick agrees that it is a "data importer" and Customer is the "data exporter" under the Model Clauses (notwithstanding that Customer may be an entity located outside of the EEA).

PART C: MISCELLANEOUS.

13. Relationship With the Agreement

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

13.2 Except for the changes made 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 patient, medical or other protected health information regulated by HIPAA or any similar U.S. federal or state laws, rules or regulations ("HIPAA Data"), if there is any conflict between this DPA and a Business Associates Agreement between Customer and Cloudwick ("BAA"), then the BAA shall prevail to extent the conflict relates to such HIPAA Data.

13.3 Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's Affiliates under this DPA shall be subject to the limitations on liability set out in the Agreement. Without limiting either of the parties' obligations under the Agreement, Customer agrees that any regulatory penalties incurred by Cloudwick in relation to the Customer Personal Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Cloudwick's liability under the Agreement as if it were liability to the Customer under the Agreement.

13.4 Any claims against Cloudwick or its Affiliates under this DPA shall only be brought by the Customer entity that is a party to the Agreement against the Cloudwick entity that is a party to the Agreement. In no event shall this DPA or any party restrict or limit the rights of any data subject or of any competent supervisory authority.

13.5 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

ANNEX A - LIST OF CLOUDWICK SUB-PROCESSORS

Cloudwick uses its Affiliates and a range of third party Sub-processors to assist it in providing the Services (as described in the Agreement). These Sub-processors as of the Effective Date of this DPA are set out below.

Entity Name: Amazon Web Services, Inc.

Corporate Location: Seattle, WA – USA

ANNEX B – SECURITY MEASURES

The security measures Cloudwick implements to protect Customer Personal Data are set out in Cloudwick's Security Policy.

ANNEX C - MODEL CLAUSES

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 sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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. Confidential

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 sub-processor 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 sub-processor 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 sub-processor 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; Page 13 of 18 Cloudwick-Customer DPA (GDPR Version) 2018May16 Cloudwick Confidential

(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 sub-processing 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 sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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;

(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 sub-processing, 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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. Sub-processing

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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.

11.3 The provisions relating to data protection aspects for sub-processing 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 sub-processing 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 sub-processor 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 sub-processor 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 the US headquartered company, Cloudwick Inc. ("Cloudwick"). Cloudwick 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 3.4 (Details of Processing) of DPA for a description of the 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 Annex B of the DPA, which describes the technical and organizational security measures implemented by Cloudwick.

Appendix 3 to the Standard Contractual Clauses

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

This Appendix 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. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.

2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, 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.

3. If the data exporter intends to suspend the transfer of personal data and/or terminate these 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").

4. 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 (Security Reports and Audits) of the DPA.

Clause 5(J): Disclosure of Sub-processor Agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward sub-processor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to sub-processor confidentiality restrictions, data importer may be restricted from disclosing onward sub-processor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any sub-processor it appoints to permit it to disclose the sub-processor agreement to data exporter.

3. Even where data importer cannot disclose a sub-processor 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 sub-processing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but to limited to, the exclusions and limitations set forth 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 7: Onward Sub-processing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward sub-processing by the data importer.

2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward sub-processors. Such consent is conditional on data importer's compliance with the requirements set out in Section 4 (Sub-processing) and Section 11 (Changes to Sub-processors) of the DPA.