DATA PROCESSING ADDENDUM

PART I - GENERAL

1. INTRODUCTION

1.1. This Data Processing Addendum ("**DPA**") forms part of the Terms of Service for the purchase of cloud services from Zadara (identified either as "**Services**" or otherwise in the applicable agreement, and hereinafter defined as "**Services**") (the "**Agreement**") and shall govern the Processing of Personal Data.

1.2. By accepting the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Zadara processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

1.3. In the course of providing the Services to Customer pursuant to the Agreement, Zadara may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

2. HOW THIS DPA APPLIES

2.1. If the Customer entity entering into this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Zadara entity that is party to the Agreement is party to this DPA. If Customer has purchased the Services through an authorized reseller, Customer should contact the authorized reseller to discuss whether any amendment to its agreement with the authorized reseller is required.

2.2. This DPA consists of two parts: the main body of the DPA, and Schedules 1 and 2.

2.3. This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in the Agreement.

PART II - DATA PROCESSING TERMS

1. DEFINITIONS

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

b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Zadara but has not signed its own Order Form with Zadara and is not a "Customer" as defined under the Agreement.

c) "**Zadara**" means Zadara Ltd., a limited liability company organized under the laws of the State of Israel, acting on its behalf and in the name and on behalf of each of its Affiliates.

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

e) "**Customer Data**" means what is defined in the Agreement as "Customer Data".

f) "**End User**" means any Data Subject who is authorized by the Customer to use the Services.

g) "**Data Protection Laws and Regulations**" means (i) laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement, and (ii) the California Consumer Privacy Act of 2018 ("CCPA"), Cal. Civ. Code 1798.1001798.199, and any amendment, modification, or revision to the CCPA.

a) "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

b) "**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

c) "**Personal Data**" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data.

d) "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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

f) "**Security Documentation**" means the Security Documentation applicable to the specific Services purchased by Customer, as updated from time to time, and accessible via Zadara's webpage, or as otherwise made reasonably available by Zadara.

g) "**Standard Contractual Clauses**" means the model clauses for a data transfer from an EU controller to a non-EU processor, adopted by the European Commission under Decision 2010/87/EU attached as Schedule 2 to this DPA.

h) "**Sub-processor**" means any entity engaged by another entity which is a Processor of Personal Data; to perform that Processor's data processing obligations on that Processor's behalf.

i) "**Supervisory Authority**" means an independent public authority established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller (or Processor), Zadara is the Processor (or Sub-Processor) and that Zadara or its Affiliates will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2 **Customer's Processing of Personal Data.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations Customer declares that Personal Data processed through the Services, was obtained and is provided to Zadara lawfully, in accordance with all requirements of Data Protection Laws and Regulations and that there is a documented legal basis for the Processing of Customer Personal Data by Zadara. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the means by which Customer acquired Personal Data and for obtaining all consents from Data Subjects whose Personal Data is included in the Customer Data and providing all notices required to be provided to such Data Subjects; prior to the Processing by Zadara. Zadara shall inform the Customer if, in its opinion, any instruction regarding the demonstration of Zadara's compliance with the Agreement infringes upon any Data Protection Law.

2.3 **Zadara's Processing of Personal Data.** Subject to the Agreement with Customer, Zadara shall Process Personal Data in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) enabling Processing by Customers and End Users in their use if the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. To the extent that Zadara cannot comply with a change to Customer's instructions without incurring material additional costs, Zadara shall: (i) inform Customer, giving full details of the problem; and (ii) continue storing the Customer Data until revised instructions are received. Any changes in Customer's instructions that affect the pricing structure or commercial relationship between the parties must go through an appropriate change procedure and approved by Zadara. The Parties confirm that this DPA is Customer's complete and final instructions to Zadara in relation to processing of the Customer Data.

2.4 **Details of the Processing.** The subject-matter of Processing of Personal Data by Zadara is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1(Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 **Data Subject Request.** Zadara shall, to the extent legally permitted, promptly notify Customer if Zadara receives a request from a Data Subject to exercise any Data Subjects' rights in accordance with the Data Protection Laws and Regulations **("Data Subject Request**"). However, it is agreed that Zadara processes only the Personal Data that Customer has chosen to share with Zadara. Zadara has no direct or contractual relationship with Data Subjects. As a result, Customer is solely responsible for satisfying all legal obligations owed directly to the Data Subject under applicable Data Protection Laws and Regulations. To the extent Zadara has Customer Personal Data that is inaccessible to or unmodifiable by Customer, Zadara will assist the Customer in responding to Data Subject Requests.

3.2 It is the Customer's responsibility to ensure that Personal Data it collects can be legally collected in the country of origin. The Customer is also responsible for providing to the Data Subject any notices required by applicable law and for responding appropriately to the Data Subject's request to exercise his or her rights with respect to Personal Data. In addition, the Customer is responsible for ensuring that its use of the Services is consistent with any privacy policy the Customer has established and any notices it has provided to Data Subjects.

3.3 Zadara will cooperate with Customer in the event the Customer initiates a data protection impact assessment, taking into account the nature of processing and information available to Zadara.

4. ZADARA PERSONNEL

4.1 **Confidentiality.** Zadara shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, and have executed written confidentiality agreements. Zadara shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 **Limitation of Access.** Zadara shall ensure that Zadara's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. SUB-PROCESSORS

5.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that Zadara may engage third-party Sub-processors in connection with the provision of the Services. Where a Sub-processor will process Personal Data which is subject to EU Data Protection Laws and Regulations, Zadara will ensure that the Sub-processor is subject to contractual obligations regarding Personal Data essentially

similar to those in this Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 **List of Current Sub-processors and Notification of New Sub-processors.** Customer may find on Zadara's webpage a mechanism to subscribe to notifications of new Sub-processors, to which Customer shall subscribe, and if Customer subscribes, Zadara shall provide notification of any new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the Services.

5.3 **Objection Right for New Sub-processors.** Customer may object to Zadara's use of a new Sub-processor by notifying Zadara promptly in writing within ten (10) business days after receipt of Zadara's notice in accordance with the mechanism set out in Section 5.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Zadara will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Zadara is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer's sole remedy is to terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Zadara without the use of the objected-to new Sub-processor by providing written notice to Zadara.

5.4 **Liability.** Zadara shall be liable for the acts and omissions of its Sub-processors to the same extent Zadara would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY

6.1 **Controls for the Protection of Customer Data.** Zadara shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the Security Documentation. Zadara regularly monitors compliance with these measures. Zadara reserves the right to modify the technical and organizational measures and/or the Security Documentation; without further notice to the Customer, provided that Zadara will not materially decrease the overall security of the Services during a subscription term. Customer is solely responsible for reviewing the information made available by Zadara relating to data security and making an independent determination as to whether the Services meet Customer's requirements, and for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding the Customer's data security responsibilities when using the Services.

7. AUDITS

7.1 **Customer Audits:**

7.1.1 The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site or remote audit of the procedures relevant to the protection of Personal Data (an "**Audit**"), take all reasonable measures to limit any impact on Zadara and its Sub-Processors.

7.1.2 The Audit shall be conducted subject to the following conditions: i) Audits shall not be more frequent than once per year; ii) the Audit shall be at the Customer's sole expense; iii) the Customer shall provide at least 30 days prior written notice of its intention to conduct an Audit and the time of the Audit shall be coordinated to both Parties convenience and at Zadara's regular working hours; iv) the Customer and any auditor appointed on Customer's behalf to perform the Audit (and which was approved by Zadara and is not a competitor of Zadara) shall: (a) sign a confidentiality undertaking which shall cover any information

relating the Audit, including the Audit results; and (b) abide Zadara's security procedures at all times; and iv) Zadara shall be entitled to restrict access to its premises and systems and to redact information from documents; in order to protect proprietary and/or confidential information of Zadara and/or any third party which Zadara is obligated to protect and which is not related to the Services.

7.1.3 Solely the Customer entity which has signed an Agreement with Zadara shall be entitled to conduct an Audit and for avoidance of doubt, Authorized Affiliates shall not be entitled to conduct any Audit. Customer may share the Audit results with Authorized Affiliates provided that each Authorized Affiliate which shall receive the Audit report shall sign a confidentiality undertaking which covers any information relating the Audit, including the Audit results.

7.2 **Third-Party Certifications and Audits.** Zadara has obtained third-party certifications and audits as set forth in the "Third-Party Certifications and Audits" section available in Zadara's website at https://www.zadara.com/platform/compliance/. Upon Customer's written request at reasonable intervals but no more than once per year, and subject to the confidentiality obligations set forth in the Agreement or as requested by Zadara at the time of disclosure, Zadara shall make available to Customer that is not a competitor of Zadara (or Customer's independent, third-party auditor that is not a competitor of Zadara), a copy of Zadara's then most recent third-party audits or certifications, as applicable.

8. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

Zadara maintains security incident management policies and procedures specified in the Security Documentation and, to the extent required under applicable Data Protection Laws and Regulations, shall notify Customer without undue delay after becoming aware of an actual unauthorized disclosure of or access to Customer Data, or compromise of Zadara's systems that Zadara determines is reasonably likely to result in such disclosure or access, caused by failure of Zadara's security measures but excluding any unauthorized disclosure or access that is caused by Customer or its End Users, including Customer or its End Users' failure to adequately secure equipment or accounts (a "**Customer Data Incident**"). Zadara shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Zadara deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Zadara's reasonable control. Zadara may limit the scope of, or refrain from delivering, any disclosures to the extent reasonably necessary to avoid compromising the integrity of Zadara's security, an ongoing investigation, or any Customer's or End User's data. Zadara will cooperate with Customers in the event of a Personal Data breach, taking into account the nature of processing and information available to Zadara.

9. RETURN AND DELETION OF CUSTOMER DATA

Subject to the Agreement, Zadara shall, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in applicable Data Protection Laws and Regulations.

10. AUTHORIZED AFFILIATES

10.1 **Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Zadara and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 10 and Section 11. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the

Services and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

10.2 **Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Zadara under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10.3 **Rights of Authorized Affiliates.** Where an Authorized Affiliate becomes a party to this DPA with Zadara, it shall, to the extent required under applicable Data Protection Laws and Regulations, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

10.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Zadara directly by itself, the parties agree that: (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section7.1 above).

11. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Zadara, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, Zadara's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Appendices (if any).

12. DATA TRANSFER

12.1 Customer may specify the Zadara region where Customer Data will be Processed within the Zadara datacenters. Once Customer has made its choice, Zadara will not transfer Customer Data from Customer's selected region, except as necessary to comply with the law or a valid and binding order of a law enforcement agency.

12.2 Zadara shall only transfer Personal Data to a sub-processor located outside of the European Economic Area (without prejudice to Section 5), subject to one of the following legal mechanisms:

(a) the requirement for Zadara to execute or procure that the sub-processor execute to the benefit of the Customer the Standard Contractual Clauses as set out in Schedule 2 with the recipient;

(b) any other specifically approved safeguard for data transfers (as recognized under EU Data Protection Laws) and/or a European Commission finding of adequacy.

12.3 The following terms shall apply to the Standard Contractual Clauses set out in Schedule 2:

(a) The Customer may exercise its right of audit under Section 5(a)vi of the Standard Contractual Clauses as set out in, and subject to the requirements of Section 7.27.1 of this DPA; and

(b) Zadara may appoint sub-processors as set out, and subject to the requirements of, Section 5 of this DPA.

(c) The governing law and jurisdiction under the Standard Contractual Clauses shall be those of the country of the data exporter in the EU.

13. LEGAL EFFECT

This DPA shall only become legally binding between Customer and Zadara when the Agreement becomes legally binding between the Parties.

List of Schedules

- **SCHEDULE 1 – DETAILS OF THE PROCESSING**
- **SCHEDULE 2 – STANDARD CONTRACTUAL CLAUSES**

SCHEDULE 1 - DETAILS OF THE PROCESSING

Subject Matter of the Personal Data Processing: The provision of the Services by Zadara to Customer.

Duration of the Personal Data Processing: The duration of the provision of Services.

Nature and Purpose of the Personal Data Processing: To enable Customer to receive and Zadara to provide the storage Services.

Categories of Personal Data: The Personal Data relating to individuals which is uploaded on to the Services by Customer or its users in their sole discretion. Zadara will process all types and categories of Personal Data uploaded by the Customer in accordance with the Agreement. Given the nature of the Services, Customer acknowledges that Zadara is not able to verify or maintain the types and categories of Personal Data. Therefore, Customer is responsible for providing complete, accurate, and up-to-date information to Zadara on the actual types and categories of Personal Data that Customer will process in the Services via instructions to Zadara as set out in the DPA.

Data Subjects: Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which includes, the following categories of data subjects:

- *Customer's users authorized by Customer to use the Services;*
- *Employees, agents, advisors, freelancers of Customer (who are natural persons);*
- *Prospects, customers, business partners and vendors of Customer (who are natural persons); and*
- *Employees or contact persons of Customer's prospects, customers, business partners and vendors.*

Zadara will process Personal Data of all data subjects listed above in accordance with the Agreement and DPA. Given the nature of the Services, Customer acknowledges that Zadara is not able to verify or maintain the above list of categories of data subjects. Therefore, if Customer will not use the Services with all the data subjects as set out above, then Customer is responsible for providing complete, accurate, and up-to-date information to Zadara on the actual data subjects from within the above list that Customer will process in the Services via instructions to Zadara as set out in the DPA.

SCHEDULE 2 – STANDARD CONTRACTUAL CLAUSES

EU 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 entity identified as "Customer" in the DPA (the "**Data Exporter**")

And
Name of the data importing organization**: Zadara Inc.**
Address: 6 Venture, Suite 140 Irvine, CA 92618, USA
Email: Support@zadarastorage.com

Or
Name of the data importing organization**: Zadara Technologies India Private Limited**
Email: Support@zadarastorage.com

(the "**Data Importer**")
each a "**party**"; together "**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.

AGREED TERMS

1. Definitions

For the purposes of the Clauses:

(a) "**personal data**", "**special categories of data**", "**process/Processing**", "**controller**", "**processor**", "**data subject**" and "**supervisory authority**" shall have the same meaning as in EU Data Protection Laws 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;

(b) the "**data exporter**" means the entity who transfers the personal data;

(c) 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 EU Data Protection Laws 95/46/EC;

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

(e) 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; and

(f) "**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 Processing.** The details of the processing and in particular the special categories of personal data where applicable are specified in Schedule 1 which forms an integral part of the Clauses.
3. **Third-party beneficiary Section**
   (a) The data subject can enforce against the data exporter this Section, Section 4(a)ii to 4(a)ix, Section 5(a)i to 5(a)v, and 5(a)vii to 5(a)x, Section 6(a) and 6(b), Section 7, Section 8(b), and Sections 9 to 12 as third-party beneficiary.
   (b) The data subject can enforce against the data importer this Section, Section 5(a)i to 5(a)v, and 5(a)vii, Section 6, Section 7, Section 8(b), and Sections 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.
   (c) The data subject can enforce against the sub-processor this Section, Section 5(a) to (e) and (g), Section 6, Section 7, Section 8(2), and Sections 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.
   (d) 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**
   (a) The data exporter agrees and warrants:
      i. 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;
      ii. 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;
      iii. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Schedule 2 to this contract;
      iv. 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;
      v. that it will ensure compliance with the security measures;
      vi. 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 EU Data Protection Laws 95/46/EC;

vii. to forward any notification received from the data importer or any sub-processor pursuant to Section 5(a)ii and Section 8(c) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

viii. to make available to the data subjects upon request a copy of the Clauses, with the exception of Schedule 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;

ix. that, in the event of sub-Processing, the Processing activity is carried out in accordance with Section 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

x. that it will ensure compliance with Section 4(a)i to (ix).

5. Obligations of the data importer

(a) The data importer agrees and warrants:

i. 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;

ii. 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;

iii. that it has implemented the technical and organisational security measures specified in Schedule 2 before Processing the personal data transferred;

iv. that it will promptly notify the data exporter about:

(a) 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;

(b) any accidental or unauthorised access; and

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

v. 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;

vi. 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;

vii. 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 Schedule 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;

viii. that, in the event of sub-Processing, it has previously informed the data exporter and obtained its prior written consent;

ix. that the Processing services by the sub-processor will be carried out in accordance with Section 11;

x. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. Liability

(a) The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Section 3 or in Section 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

(b) 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 Section 3 or in Section 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 or by operation of law, in which case the data subject can enforce its rights against such entity.

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

(c) If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs (a) and (b), arising out of a breach by the sub-processor of any of their obligations referred to in Section 3 or in Section 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

(a) 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:

i. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

ii. to refer the dispute to the courts in the Member State in which the data exporter is established.

(b) 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. Co-operation with supervisory authorities

(a) 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.

(b) 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.

(c) 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 Section 5(a)ii.

9. **Governing law.** The Clauses shall be governed by the laws 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 Section.
11. **Sub-Processing**
    (a) 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 fulfill 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.
    (b) The prior written contract between the data importer and the sub-processor shall also provide for a third party beneficiary Section as laid down in Section 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph (a) of Section 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own Processing operations under the Clauses.
    (c) 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.
    (d) The data exporter shall keep a list of sub-Processing agreements concluded under the Clauses and notified by the data importer pursuant to Section 5(a)x, 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**
    (a) 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.
    (b) 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 (a).

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER:

Customer Legal Name

Customer Signature

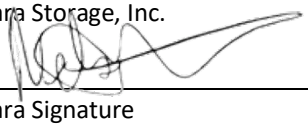
Print Name

Title

Date

ZADARA:

Zadara Storage, Inc.



Zadara Signature

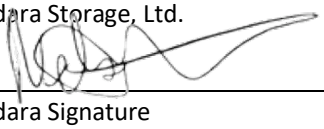
Nelson Nahum
Name

CEO
Title

Sep 15,2021
Date

ZADARA:

Zadara Storage, Ltd.



Zadara Signature

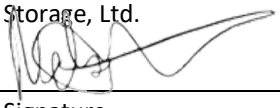
Nelson Nahum
Name

CEO
Title

Sep 15,2021
Date

ZADARA:

Zadara Storage, Ltd.



Zadara Signature

Nelson Nahum
Name

CEO
Title

Sep 15,2021
Date

Appendix 1
to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Data Exporter. The Data Exporter is the customer to the Agreement, as described in the DPA.

Data Importer. The Data Importer is Zadara Inc. and/or Zadara Technologies India Private Limited ("Zadara"), a global provider of cloud compute, storage and such other Services. storage and such other Services.

Data Subjects. The personal data transferred concern the Data Exporter's and Data Exporter's affiliates' end users including employees, consultants and contractors of the Data Exporter, as well as Data Exporter's users authorized by Data Exporter's to use the Services, prospects, customers, business partners and vendors of Data Exporter (who are natural persons), employees or contact persons of Data Exporter's prospects, customers, business partners and vendors.

Categories of data The personal data transferred concern end users identifying information and organization data (both on-line and offline) as well as documents, images and other content or data in electronic form stored or transmitted by end users via Data Importer's services.

Processing operations. The personal data transferred will be subject to the following basic processing activities through Zadara's cloud Services.

Scope of Processing. The scope and purposes of processing the Data Exporter's personal data is described in the DPA to which these Clauses are annexed as well as the Agreement between Data Exporter and Data Importer.

Term of Processing. The term for data processing will be the term set forth in the applicable Agreement.

Data Deletion or Return. Upon expiration or termination of the Agreement, Data Importer agrees to delete or return Data Exporter's personal data from Data Importer's service, in accordance with the terms and conditions of the Agreement.

Sub-processing. Data Importer may engage other companies to provide parts of the Service on Data Importer's behalf. Data Importer will ensure that any such Sub-Processors will only access and use any personal data of Data Exporter to provide the service in accordance with the Agreement.

Appendix 2
to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

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

1. **Information Security Program.** Zadara maintains an information security program designed to (a) secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable risks to security and unauthorized access to the customer data. Zadara's CISO coordinates and is accountable for the information security program. The information security program includes the following measures:

1.1. **Physical Security**

1.1.1. The Zadara Clouds are physically located in the most secure data centers of the leading Providers. As of the writing of this document, Zadara Storage is hosted at Equinix and Cyxtera data center, in locked cabinets and cages.

1.1.2. In OPaaS (On Premises) installations, the customer takes full responsibility for the physical security, physical health and access to the Zadara systems.

1.2. **Network Security**. Zadara clouds are electronically accessible to employees and any other person as necessary to provide the Services. Zadara maintain access controls and policies to manage what access is allowed to each Zadara system, each network connection and user, including the use of firewalls or equivalent technology and authentication controls. Zadara will maintain corrective action and incident response plans to respond to potential security threats.

1.3. **Secure Communication.** All management traffic, and data transfer is done over secured, encrypted communication

1.4. **Data Privacy.** The VPSA architecture grants data privacy for Zadara Users in a multi-tenant cloud environment. Including dedicated VMs and dedicated drives.

1.5. **Security Certifications.** Zadara storage services are compliant with most of common security standards and regulations. Zadara goes under annually audits to maintain the relevant certifications as set forth in the "Third-Party Certifications and Audits" section available in Zadara's website at https://www.zadara.com/platform/compliance/ .Please note that said certification may not apply to all Services. Please check each Service certification on our website before Ordering the services.

2. **Continued Evaluation.** Zadara will conduct periodic reviews of the security of its clouds and adequacy of its information security program as measured against industry security standards and its policies and procedures. Zadara will continually evaluate the security of its services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.