

DATA PROCESSING ADDENDUM (OPERATORS)

PART I - GENERAL

1. INTRODUCTION

- 1.1. This Data Processing Addendum (“**DPA**”) forms part of the Zadara Federated Edge Addendum entered into by Zadara and the Operator as part of the Zadara Partner Agreement, for the provision of the Operator Services by Operator to Zadara for hosting Zadara’s Services for the purpose of their use by Customers (hereinafter defined as “**Services**” or “**Operator Services**” and the “**Agreement**”) and shall govern the Processing of Personal Data pursuant to the Agreement.
- 1.2. In the course of providing the Services to Zadara pursuant to the Agreement, Operator may Process Personal Data on behalf of Zadara’s Customers and the Operator agrees to comply with the following provisions with respect to any Personal Data processed by Operator in performance of the Services, acting reasonably and in good faith.

2. HOW THIS DPA APPLIES

- 2.1. 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.
- 2.2. This DPA consists of two parts: the main body of the DPA, and Schedules 1 and 2.
- 2.3. This DPA shall apply to the processing of Customer Data by Operator in providing the Services to Zadara. In the event Operator is also a Partner reselling Zadara Services to its own customers, the data protection provisions contained in the Agreement shall apply in lieu of this DPA. In any conflict between this DPA and the data protection provisions contained in the Agreement, the provisions of this DPA shall prevail in relation to the subject matter of this DPA.

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 Operator’s Affiliate(s) which is permitted by Zadara in writing to provide the Services pursuant to the Agreement between Zadara and Operator as a sub-processor of Operator.
- 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, in the context of this DPA - the Customer.
- e) **“Customer”** means a person or legal entity which has signed a commercial agreement with Zadara for provision of services by Zadara, in relation to which the Operator acts as a subprocessor. It is clarified for the avoidance of doubt that the definition of “Customer” in the Agreement does not apply to this DPA.
- f) **“Customer Data”** means what is defined in the Agreement as “Customer Data”.
- g) **“End User”** means any Data Subject who is authorized to use the Services by a Customer.
- h) **“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 this DPA 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), where 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 an entity which Processes Personal Data on behalf of and under the instructions of another party, in the context of this DPA - each of Zadara and Operator.
- f) **“Security Documentation”** means the Security policies and procedures applicable to Operator’s Services, the material aspects of which are detailed in Appendix 2 to Schedule 2 including any certifications by third party auditors, which shall be made available to Zadara immediately upon request.
- 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.

Any terms not defined in the DPA are defined in the Agreement.

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, Zadara may act as a Processor or Sub-Processor to its Customers, and Operator is a Sub-Processor Processing Personal Data on behalf of Zadara.
- 2.2 **Operator’s Processing of Personal Data.** Subject to the Agreement and execution of the Zadara Federated Edge Addendum, Operator shall Process Personal Data in accordance with Zadara’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement as required to perform the Operator Services; and (ii) Processing to comply with other documented instructions provided by Zadara. To the extent that Operator cannot comply with a change to Zadara’s instructions because it is prohibited under applicable law, Operator shall: (i) promptly inform Zadara, giving full details of the problem; and (ii) continue to store the Personal Data until revised instructions are received.
- 2.3 **Details of the Processing.** The subject-matter of Processing of Personal Data by Operator is the performance of the Operator 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.** Operator shall notify Zadara without undue delay and no later than three (3) business days from the moment it receives a request from a Data Subject to exercise any Data Subjects’ rights as defined under Data Protection Laws and Regulations (a **“Data Subject Request”**). With respect to such Data Subject Request, Operator shall: i) forward the Data Subject Request to Zadara and any related information available to Operator; ii) not respond or take any action in relation to the Data Subject Request except as requested in writing by Zadara; iii) reasonably cooperate with Zadara’s written instructions in relation to the Data Subject Request assist Zadara in responding to Data Subject

Requests; and iv) maintain a record of Data Subject Requests handled by Operator including only the minimal Personal Data required to demonstrate compliance with Data Subjects' rights, attend to any further inquiries by Data Subjects, and shall limit access to such records to relevant personnel only.

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

4. OPERATOR PERSONNEL

- 4.1 **Confidentiality.** Operator shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Operator shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

- 4.2 **Reliability.** Operator shall take commercially reasonable steps to ensure the reliability of any Operator personnel engaged in the Processing of Personal Data.

- 4.3 **Limitation of Access.** Operator shall ensure that Operator's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement and on a "need to know" basis.

5. OPERATOR SUB-PROCESSORS

- 5.1 **Appointment of Sub-processors.** Operator may engage third-party Sub-processors in connection with the provision of the Services only subject to the prior written approval of Zadara. Operator will ensure that the Sub-processor is subject to contractual obligations regarding Personal Data no less protective than those set out in this Agreement with respect to the protection of Personal Data and in full compliance with the Data Protection Laws and Regulations.

- 5.2 **List of Current Sub-processors and Notification of New Sub-processors.** The list of Operator's current Subprocessors is included in Schedule 3 of this DPA. Operator shall provide notification of any new Sub-processor(s) at least thirty (30) days before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the Services with all relevant details in order to enable Zadara to review and approve or reject the new Subprocessor.

- 5.3 **Objection Right for New Sub-processors.** Zadara may object to Operator's use of a new Sub-processor by notifying Operator promptly in writing within fourteen (14) business days after receipt of Operator's notice in accordance with the mechanism set out in Section 5.2. In the event Zadara objects to a new Sub-processor, as permitted in the preceding sentence, Operator will use reasonable efforts to make available to Zadara a change in the Services or recommend another Sub-processor or perform the Services to avoid Processing of Personal Data by the objected-to new Sub-processor. If Operator is unable to make available such change within a reasonable period of time, Operator may not use

such new Sub-processor.

- 5.4 **Authorized Affiliates.** Operator's Authorized Affiliates shall be deemed Subprocessors for the purpose of this DPA.
- 5.5 **Liability.** Operator shall be fully liable for the acts and omissions of its Sub-processors to the same extent Operator would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY

- 6.1 **Controls for the Protection of Customer Data.** Operator 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, and not less than as set forth in Appendix 2 to Schedule 2. Operator shall regularly monitor compliance with these measures. Operator will not modify technical and organizational measures during the term of the Agreement, except for updates in existing data security applications which enhance security and shall not the decrease the overall security of the Services during the term of the Agreement.
- 6.2 **Third-Party Certifications and Audits.** Operator is required to have completed the minimum required certifications detailed in Annex A of the Agreement, by an independent auditor that has evaluated the design and effectiveness of Operator's security policies, procedures, and controls, prior to the commencement of the Services. Operator will continue to undergo regular audits for the Services during the term of the Agreement and keep its certifications valid consecutively throughout the term of the Agreement. Upon Zadara's written request at reasonable intervals, but no more than once per year, and subject to the confidentiality obligations set forth in the Agreement, Operator shall make available to Zadara a copy of Operator's then most recent third-party audits or certifications, as applicable.

7. AUDITS

- 7.1 Zadara shall be entitled to carry out an on-site or remote audit and inspection of Operator's premises, systems and documents upon which Customer Data is processed. Operator shall reasonably assist by enabling Zadara and/or an auditor mandated by Zadara at its sole discretion to access the relevant information, systems and infrastructure in order enable Zadara to duly assess Operator's compliance with the Data Protection Laws and Regulations and this DPA. Operator shall not unreasonably restrict access to its premises and systems in a manner obstructs the performance of the audit.
- 7.2 The audit shall be conducted no more than once per year from the commencement of this DPA, following reasonable prior notice, at Operator's business hours; except if the audit is requested immediately following a Security

Incident.

- 7.3 To the extent Operator receives any report or certification relating to data security and privacy of a Subprocessor, Operator shall share the report or certification with Zadara.

8. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

- 8.1 Operator shall maintain 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 Zadara without undue delay and no later than 24 hours after becoming aware of any actual or reasonably suspected unauthorized disclosure of or access to Customer Data, or compromise of Operator's systems that may result in such disclosure or access (a "Security Incident").
- 8.2 In the aforementioned notification to Zadara, Operator shall provide the following information: i) the number and categories of Data Subjects and records affected by the Security Incident; ii) the number and categories of Personal Data affected by the Security Incident; iii) the causes for the Security Incident and all measures taken to investigate and remediate the Security Incident. If the information is not available to Operator at the time of notification, Operator shall update the notification immediately upon the discovery of additional information, including reasons for the delay. Unless required by applicable laws, Operator shall not report the Security Incident to any governmental authority and/or Data Subject without the prior written approval of Zadara.
- 8.3 Operator shall initiate an investigation of the Security Incident and make best efforts to identify the cause of such Security Incident and take all necessary steps in order to remediate the cause of such a Security Incident, including implementation of any instructions received from Zadara. Operator shall document the investigation and its findings and all remediation steps taken by Operator.

9. RETURN AND DELETION OF CUSTOMER DATA

To the extent that Operator has access to the Customer Data, subject to the Agreement, Operator shall, to the extent allowed by applicable law, and at Zadara's request, delete Customer Data in its possession in accordance with the procedures and timeframes specified in applicable Data Protection Laws and Regulations or as required by Zadara in writing. If required by Zadara, Operator shall first transfer the Customer Data to Zadara in a secure manner of Zadara's choice and after confirmation by Zadara that all Customer Data has been received, Operator shall permanently delete the Customer Data from its systems including backups; such that it cannot be retrieved and certify such deletion in writing to Zadara.

10. DATA TRANSFER

- 10.1 Operator will not transfer Customer Data, except as necessary to comply with

mandatory law or a valid and binding order of a law enforcement agency, in which latter case Operator shall notify Zadara immediately in writing.

- 10.2 Operator 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) execution of 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.
- 10.3 The following terms shall apply to the standard contractual Sections set out in Schedule 2: the governing law and jurisdiction under the Standard Contractual Clauses shall be those of the country of the data exporter in the EU.

11. LEGAL EFFECT

This DPA shall only become legally binding between Operator 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 3 – LIST OF SUBPROCESSORS**

SCHEDULE 1 - DETAILS OF THE PROCESSING

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

Duration of the Personal Data Processing: The term of the Agreement, and any period after the term of the Agreement prior to Operator's deletion of Customer Data.

Nature and Purpose of the Personal Data Processing: To enable Operator to provide the Operator Services.

Categories of Personal Data: The Personal Data relating to individuals which is uploaded on to the Services by Customer or its End Users.

Data Subjects: Customer may submit Personal Data to the Services, which may include, but is not limited to Personal Data relating to the following categories of data subjects:

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

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.

Name of the data exporting organization:

Zadara Inc.

Address: 6 Venture, Suite 140 Irvine, CA 92618, USA

Email: Support@zadarastorage.com

(the “**Data Exporter**”)

And

Name of the data importing organization: The entity identified as “Operator” in the DPA

(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

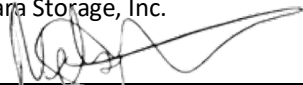
Print Name

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

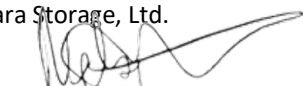
Title

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 Zadara Ltd. and/or Zadara UK Limited and/or Zadara Inc. and/or Zadara Technologies Ltd. and/or Zadara Technologies India Private Limited and/or Zadara KK (“Zadara”), a global provider of cloud compute, storage and such other Services.

Data Importer. The Data Importer is the Operator defined in the DPA, a provider of hosting services as further described in the Agreement.

Data Subjects. The Personal Data transferred concerns the Data Exporter’s and Data Exporter’s or its affiliates’ customers and their end users including employees, consultants and contractors of such customers, 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 the Operating Services: hosting Zadara's Compute, storage and such other Services and processing of Customer Data on Zadara's behalf, provision of physical security, rack space, power supply, climate control and other 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 return Data Exporter’s personal data, 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 subject to the terms of the DPA. 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 and must be completed by the parties.

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.** Operator 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. Operator's CISO coordinates and is accountable for the information security program. The information security program includes the following measures:
2. **Physical Security.** The datacenter owned or licensed by Operator shall meet Zadara's Minimum Certifications and/or Capabilities defined in the Agreement, including but not limited:
 - 2.1. Building Perimeter Security: Monitoring all entrances and exits 7x24.
 - 2.2. Access Control: Visitors authorization, biometric/access card readers, video monitoring.
 - 2.3. Dedicated cages/locked racks for Zadara Equipment, restricted only to authorized personnel by means of an additional card reader or biometric scanner on the cage door.
 - 2.4. Access to the cages requires Zadara's approval of authorized personnel.
3. **Network Security.** Operator clouds are electronically accessible to Zadara employees and any other person as necessary to provide the Services. Operator maintain access controls and policies to manage what access is allowed to each Operator system, each network connection and user, including the use of firewalls or equivalent technology and authentication controls.
4. **Secure Communication.** All management traffic, and data transfer is done over secured, encrypted communication
5. Operator will maintain corrective action and incident response plans to respond to potential security threats.
6. **Security Certifications.** Operator services are compliant with most of common security standards and regulations. Operator goes under annually audits to maintain the minimum relevant certifications as set forth below, and any other certification which apply to the Services, as advised by the Operator:
 - **Security Required Certifications** - SOC2 Type2 or ISO27001
 - **Data Privacy** - GDPR /CCPA/other local privacy regulations compliance (whatever applicable)
 - **Datacenter Reliability**
Capabilities comparable to Tier 3 and Tier 4 datacenters.

	Tier 3	Tier 4
Allowed Downtime (hours/year)	1.6	0.5
Guaranteed availability (%)	99.98	99.995
Power	Multiple	Multiple
Cooling	Multiple	Multiple
Redundancy	N+1	2N+1
Sustain power outage (h)	72	96

7. **Continued Evaluation.** Operator 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. Operator 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.

Schedule 3
List of Sub processors

List of Subprocessors

Name of Subprocessor	Nature of Services	Geographic location and processing location	comments