Last updated: August, 2023

DATA PROCESSING AGREEMENT

This Data Processing Addendum ("**Addendum**") is incorporated in to the Terms of Service and Service Order(s) ("**Agreement**") executed by and between the service provider signing the Agreement ("**Service Provider**") and Growth Space entity executing the Agreement ("**Company**") (each, a "**Party**" and, collectively, the "**Parties**") and shall apply automatically upon signature of the Agreement. In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement.

1. DEFINITIONS

1.1 In this Addendum, the following terms shall have the meanings set out below:

1.1.1 "**Authorised Subprocessors**" means (a) those Subprocessors set out in Schedule 3 (Authorised Subprocessors); and (b) any additional Subprocessors consented to in writing by Company in accordance with Section 6.1;

1.1.2 "**Data Protection Laws**" shall mean applicable privacy law with respect to the Processing of any Company Personal Data, including, without limitation, Directive 95/46/EC and Directive 2002/58/EC, in each case as transposed into domestic legislation of each Member State of the European Economic Area and in each case as amended, replaced or superseded from time to time, including without limitation by the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("**GDPR**" and collectively with the foregoing "**EU Data Protection Laws**"), any data protection laws substantially amending, replacing or superseding the GDPR, the United Kingdom General Data Protection Regulation ("**UK-GDPR**"), and the data protection or privacy laws of any other country including, without limitation, the United States of America (federal and state privacy and security laws), including, without limitation, the California Consumer Privacy Act of 2018, Cal. Civil Code Title 1.81.5 and the regulations and amendments (including the California Privacy Rights Act) thereunder ("**CCPA**"); the Privacy Law – 1981 and any regulations enacted thereunder including the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761-2001 and Privacy Protection Regulations (Data Security), 5777-2017, and any guidelines and/or instructions published by the Israeli Privacy Protection Authority;

1.1.3 **"Delete**" means the removal or obliteration of Personal Data such that it cannot be recovered or reconstructed;

1.1.4 **"EEA**" means the European Economic Area;

1.1.5 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.6 **"Company Personal Data**" means the data described in Schedule 1 and any other confidential information and/or Personal Data Processed by Service Provider or any Service Provider Affiliate on behalf of Company or any Company Affiliate pursuant to or in connection with the Agreement or provided by Company or any Company Affiliate to Service Provider or any Service Provider Affiliate. For clarity, Company Personal Data also includes any personal data available or hosted on Company's databases or Company-controller databases;

1.1.7 "**Mandated Auditor**" has the meaning given to it in Section 11;

1.1.8 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Company Personal Data transmitted, stored or otherwise Processed, as well as any breach of Section 5 of this Addendum, or of the data protection, confidentiality or security provisions of the Agreement or as such term or substantially equivalent term may be defined in Data Protection Laws;

1.1.9 "**Process/Processing**", "**Data Controller**", "**Data Processor**", "**Data Subject**", **"Personal Data", "Personal Information",** and "**Special Categories of Personal Data**" shall have the same meaning that such term or substantially equivalent term may be defined in Data Protection Laws;

1.1.10 "**Relevant Date**" means the date falling on the earlier of (i) the cessation of Processing of Company Personal Data by Service Provider or Service Provider Affiliates; or (ii) termination of the Agreement;

1.1.11 "**Restricted Transfer**" means either (i) a transfer of Personal Data from Company or any Company Affiliate ("**Transferor**") to Service Provider or any Service Provider Affiliate ("**Transferee**"); or (ii) an onward transfer from Service Provider or Service Provider Affiliate to a Subprocessor (also a "**Transferee**"), in each case where such transfer would be prohibited by Data Protection Laws in the absence of the Standard Contractual Clauses to be established under Section 12 below or, in jurisdictions where Standard Contractual Clauses are not recognized, such transfer would be prohibited by Data Protection Laws if a mechanism offering sufficient safeguards on data protection for data to be transferred, as set forth in the applicable Data

Protection Laws was not implemented. For clarity, where a transfer of Personal Data from one country to another country is of a type authorised by Data Protection Laws in the exporting country for example in the case of transfers from within the European Union to a country or scheme which is approved by the European Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer for the purposes of this Addendum;

1.1.12 "**Services**" means the services to be supplied by Service Provider and/or Service Provider Affiliates to Company and/or Company Affiliates pursuant to the Agreement;

1.1.13 "**Standard Contractual Clauses**" means (i) the standard contractual clauses for the transfer of Personal Data to Data processors established in third countries which do not ensure an adequate level of protection as set out in Regulation (EU) 2016/679 of the European Parliament and of the Council from June 4, 2021, as available here, as updated, amended, replaced or superseded from time to time by the European Commission; or (ii) where required from time to time by a Supervisory Authority for use with respect to any specific Restricted Transfer, any other set of contractual clauses or other similar mechanism approved by such Supervisory Authority or by Data Protection Laws for use in respect of such Restricted Transfer, as updated, amended, replaced or superseded from time to time by such Regulatory Authority or Data Protection Laws;

1.1.14 **"Subprocessor**" means any Data Processor (including any third party and any Service Provider Affiliate) appointed by Service Provider to Process Company Personal Data on behalf of Company or any Company Affiliate;

1.1.15 "**Supervisory Authority**" means (a) an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws;

1.1.16 "**Service Provider Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Service Provider, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.17 "**UK GDPR**" means the Data Protection Act 2018, as updated, amended, replaced or superseded from time to time by the ICO; and

1.1.18 **"UK Standard Contractual Clauses" or "UK SCCs"** means the standard contractual clauses for the transfer of Personal Data to Data processors established in third countries which do not ensure an adequate level of protection as set out by the ICO, as available here, as updated, amended, replaced or superseded from time to time by the ICO.

1.2 The terms used in this Addendum shall have the meanings set forth herein. Except as modified below, the terms of the Agreement shall remain in full force and effect.

2. SUBJECT MATTER

2.1 In the course of providing the Services to Company and Company Affiliates pursuant to the Agreement, Service Provider and Service Provider Affiliates may Process Company Personal Data on behalf of Company or any Company Affiliate. Service Provider agrees to comply with the provisions set out in this Addendum, the Agreement and Data Protection Laws with respect to any Company Personal Data submitted by or for Company or any Company Affiliate to the Services or otherwise collected and Processed or handled on behalf of, or for the benefit for, Company or any Company Affiliate by Service Provider or any Service Provider Affiliate.

2.2 Service Provider represents and warrants that, as of the Addendum Effective Date, it provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing of Company Personal Data will meet the requirements of the GDPR and ensure the protection of the rights of the Data Subjects.

3. PROCESSING OF COMPANY PERSONAL DATA

3.1 Service Provider shall only Process the types of Company Personal Data relating to the categories of Data Subjects for the purposes and systems to which Service Provider shall have access to, of the Agreement and for the specific purposes in each case as set out in Schedule 1 to this Addendum and shall not Process, transfer, modify, amend or alter the Company Personal Data or disclose or permit the disclosure of the Company Personal Data to any third party other than in accordance with Company's documented instructions (whether in the Agreement, this Addendum or otherwise) unless such Processing is required by Data Protection Laws to which Service Provider is subject, in which case Service Provider shall to the extent permitted by Data Protection Laws inform Company of that legal requirement before Processing that Personal Data and unless prohibited to do so by specific provisions of Data Protection Laws, Service Provider shall seek Company's prior written consent before such Processing operation.

3.2 For the purposes set out in Section 3.1 above, Company hereby instructs Service Provider to transfer Company Personal Data to the recipients in the countries listed in Schedule 3 (Authorised Subprocessors List) always provided that Service Provider shall comply with Section 6 (Sub-processors) and Section 12 (Restricted Transfers).

3.3 Service Provider represents and warrants that it is not, and has never been, subject to civil or criminal litigation, or government investigation, or consent decree, judgment, or order, regarding data privacy or information security, and that

it has not suffered any material security breach or, if it has, that it has disclosed information regarding such security breach(es) to Company.

4. PERSONNEL

4.1 Service Provider shall take reasonable steps to ensure the reliability of any employee, agent or contractor of Service Provider and/or Service Provider Affiliates who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Company Personal Data, as strictly necessary for the purposes set out in Section 3.1 above in the context of that individual's duties to Service Provider, ensuring that all such individuals:

4.1.1 are informed of the confidential nature of the Company Personal Data and are aware of Service Provider's obligations under this Addendum and the Agreement in relation to the Company Personal Data;

4.1.2 have undertaken appropriate training in relation to Data Protection Laws;

4.1.3 are subject to confidentiality undertakings or professional or statutory obligations of confidentiality; and

4.1.4 are subject to user authentication processes when accessing the Company Personal Data.

5. TECHNICAL AND ORGANIZATIONAL MEASURES DPO, REPRESENTATIVE AND RECORD KEEPING

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Service Provider shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate the measures referred to in Article 32(1) of the GDPR and at the minimum the criteria specified in Schedule 4, as well as assist Company with regard to ensuring Company's compliance with its own obligations related to its security measures (including, without limitation, as required by Article 32 of the GDPR.)

5.2 In assessing the appropriate level of security, Service Provider shall take account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company Personal Data transmitted, stored or otherwise Processed.

5.3 Service Provider shall demonstrate the implementation of such measures upon Company's request.

5.4 Where Service Provider has appointed a data protection officer ("**DPO**") and/or representative for GDPR purposes ("**GDPR Representative**"), it shall communicate the name and contact details of the DPO and/or of the GDPR Representative to Company in writing (email shall suffice) 5 business days after the execution of this Addendum.

5.5 Service Provider shall comply at all times with Article 30 of the GDPR (entitled "**Records of processing activities**"). Service Provider shall provide Company with the records applicable to Company or Company Personal Data to Company upon Company's request.

6. **SUBPROCESSORS**

6.1 Subject to Section 6.3, Service Provider shall not engage any Data Processors to Process Company Personal Data other than with the prior written consent of Company, which Company may refuse in its absolute discretion.

6.2 With respect to each Subprocessor, Service Provider shall:

6.2.1 provide Company with full details of the Processing to be undertaken by each Subprocessor;

6.2.2 carry out adequate due diligence on each Subprocessor to ensure that it is capable of providing the level of protection for Company Personal Data as is required by this Addendum including without limitation sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of GDPR and this Addendum, and provide evidence of such due diligence to Company where requested by Company or a Supervisory Authority;

6.2.3 include terms in the contract between Service Provider and each Subprocessor which are the same as those set out in this Addendum. Upon request, Service Provider shall provide a copy of its agreements with Subprocessors to Company for its review;

6.2.4 insofar as that contract involves a Restricted Transfer for which Standard Contractual Clauses have not been executed, or any other mechanism enabling the Restricted Transfer pursuant to the applicable Data Protection Laws procure that each Transferee enter into such a contract with Company (or such other arrangement as may be agreed with Company), in each case in order to ensure the adequate protection of the transferred Company Personal Data; and

6.2.5 remain fully liable to Company for any failure by each Subprocessor to fulfil its obligations in relation to the Processing of any Company Personal Data.

6.3 As at the Addendum Effective Date, Company hereby authorises Service Provider to engage those Subprocessors set out in Schedule 3 (Authorised Subprocessors).

7. DATA SUBJECT RIGHTS

7.1 Taking into account the nature of the Processing, Service Provider and Service Provider Affiliates shall assist Company by implementing appropriate technical and organisational measures to facilitate the fulfilment of Company's and Company Affiliate's applicable obligation to respond to requests for exercising Data Subject rights laid down in GDPR.

7.2 Service Provider shall promptly notify Company if it receives a request from a Data Subject under any Data Protection Laws in respect of Company Personal Data.

7.3 Service Provider shall co-operate as requested by Company to enable Company to comply with any exercise of rights by a Data Subject under any Data Protection Laws in respect of Company Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws in respect of Company Personal Data or this Addendum, which shall include:

7.3.1 the provision of all data requested by Company within any reasonable timescale specified by Company in each case, including full details and copies of the complaint, communication or request and any Company Personal Data it holds in relation to a Data Subject;

7.3.2 where applicable, providing such assistance as is reasonably requested by Company to enable Company to comply with the relevant request within the timescales prescribed by the Data Protection Laws; and

7.3.3 implementing any additional technical and organisational measures as may be reasonably required by Company to allow Company to respond effectively to relevant complaints, communications or requests.

7.4 Service Provider shall (i) have a policy to duly identify and deal with Data Subject Rights requests (including identifying the request, acknowledging receipt, responding/resolving by the deadline requested by Company), (ii) promptly handle such request and provide a satisfactory response and deliverable to Company by the deadline requested by Company and (iii) ensure that the Services and systems provided by Service Provider are designed to locate the Personal Data relating to a specific individual, to rectify it, to Delete it, or to perform any other operation necessary under Data Protection Laws.

7.5 Service Provider shall ensure that Company Personal Data is separated at all times from Service Provider’s own data and Service Provider’s customers’ data.

8. PERSONAL DATA BREACH

8.1 Service Provider shall notify Company promptly and without any undue delay, and in any case within twelve (12) hours, upon becoming aware of or reasonably suspecting a Personal Data Breach providing Company with sufficient information which allows Company to meet its respective obligations Breach under the Data Protection Laws, including any obligations to report the Personal Data Breach to the competent Supervisory Authorities, and/or inform the Data Subjects Such notification shall as a minimum:

8.1.1 describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

8.1.2 communicate the name and contact details of Service Provider's data protection officer or other relevant contact from whom more information may be obtained;

8.1.3 describe the likely consequences of the Personal Data Breach; and

8.2 describe the measures taken or proposed to be taken to address the Personal Data Breach. Service Provider shall co-operate with Company and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each Personal Data Breach.

8.3 In the event of a Personal Data Breach, Service Provider shall not inform any third party (including any individuals) without first obtaining Company’s prior written consent, unless notification is required under Data Protection Law and/or by EU or Member State law to which Service Provider is subject, in which case Service Provider shall to the extent permitted by such law inform Company of that legal requirement, provide a copy of the proposed notification and consider any comments made by Company before notifying the Personal Data Breach.

8.4 Service Provider will promptly reimburse Company for all costs reasonably incurred by Company in connection with the Personal Data Breach including, but not limited to, costs related to Company's provision of notice of the Personal Data Breach to Supervisory Authorities, or affected Data Subject (if determined appropriate by Company or required by Data Protection Laws.)

9. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

9.1 Service Provider shall provide reasonable assistance to Company with any data protection impact assessments which are required under Data Protection Law and with any prior consultations to any Supervisory Authority of Company or any Company Affiliate which are required under Data Protection Law, in each case solely in relation to Processing of Company Personal Data by Service Provider on behalf of Company and taking into account the nature of the Processing and information available to Service Provider.

10. DELETION OR RETURN OF COMPANY PERSONAL DATA

10.1 Subject to Sections 10.2 and 10.3, Service Provider shall promptly and in any event within 10 (ten) calendar days of the Relevant Date: (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as notified by Company to Service Provider; and (b) Delete and procure the Deletion of all other copies of Company

Personal Data (including, automatically created archival copies) Processed by Service Provider or any Authorised Subprocessor. Service Provider shall provide written certification to Company that it has fully complied with this Section 10.1 within 10 (ten) days of the Relevant Date.

10.2 Subject to Section 10.3, Company may in its absolute discretion notify Service Provider in writing with 10 (ten) days prior notice to require Service Provider to Delete and procure the Deletion of all or any copies of Company Personal Data Processed by Service Provider or any Authorised Subprocessor. Service Provider shall provide written certification to Company that it has fully complied with this Section 10.2 within 10 (ten) days of the prior notice.

10.3 Service Provider may retain Company Personal Data to the extent required by Data Protection Laws and only to the extent and for such period as required by Data Protection Laws and always provided that Service Provider shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Data Protection Laws requiring its storage and for no other purpose. Service Provider shall defend, indemnify and hold harmless Company and Company Affiliates (including, without limitation, their directors, officers, staff, agents, subcontractors, and service providers) from any liability of any kind in connection with the retained copy, the Processing and/or the consequences thereof, and this Section 10.3 shall survive the termination of the Agreement, this Addendum and/or the Services for any reason.

11. AUDIT RIGHTS

11.1 In addition to any audit rights granted pursuant to the Agreement, Service Provider shall make available to Company on request all information necessary to demonstrate compliance with this Addendum and allow for and contribute to audits, including inspections by Company or an auditor mandated by Company or any Company Affiliate ("**Mandated Auditor**") of any premises where the Processing of Company Personal Data takes place in order to assess compliance with this Addendum. Service Provider shall permit Company or a Mandated Auditor to inspect, audit and copy any relevant records, processes, policies and systems in order that Company may satisfy itself that the provisions of this Addendum are being complied with. Service Provider shall provide full co-operation to Company in respect of any such audit and shall at the request of Company, provide Company with evidence of compliance with its obligations under this Addendum. Service Provider shall immediately inform Company if, in its opinion, an instruction pursuant to this Section 11 (Audit Rights) infringes the GDPR or other Data Protection Laws.

12. RESTRICTED TRANSFERS

12.1 With regard to transfers of Personal Data to entities located, residing or incorporated in a third country or to an international organisation (including Restricted Transfers), the Parties shall assure adequate protection for the Company Personal Data as follows:

12.1.2. If the Company transfers Personal Data outside of the EU or an adequate country, then the Company, on behalf of itself and each Company Affiliate as Transferor and Service Provider on behalf of itself and each Service Provider Affiliate as Transferee hereby enter into the Standard Contractual Clauses set out in Schedule 2.

To the extent that there is any conflict or inconsistency between the terms of the Standard Contractual Clauses and the terms of this Addendum, the terms of the Standard Contractual Clauses shall take precedence.

The Standard Contractual Clauses and/or the UK Standard Contractual Clauses shall come into effect on the commencement of a Restricted Transfer among any Parties.

In case of any Restricted Transfer, any entity of Service Provider's group, including, the Data Importer (as defined below in the SCCs) shall cause any entity receiving the Personal Data to implement sufficient guarantees and measures to protect the Personal Data and ensure that the level of protection of the SCCs, the Data Protection Laws (includes the GDPR and the UK GDPR if applicable), and Articles 7 and 8 of the European Charter of Fundamental Rights is at all times respected in the Third Country. The Data Importer hereby ensures that it is not aware of, and in any event it will immediately inform the Data Exporter (as defined below in the SCC) of, any inability to comply with the SCCs, the Data Protection Laws (includes the GDPR and the UK GDPR if applicable) and Articles 7 and 8 of the European Charter of Fundamental Rights and/or this section. Notwithstanding anything to the contrary, where protections in the recipient country of the Data Importer are not adequate, the Data Exporter (in each case) is entitled to: (i) suspend the transfer of Personal Data until the parties have solved the issue, (ii) request the deletion of the Personal data, which Data Importer shall immediately and permanently delete and not disclose to any third party, and/or (iii) immediately terminate the Agreement with the Data Importer with respect to the affected Processing.

The Data Importer hereby represents, warrants and covenants that: (i) no law, regulation and/or government policy applicable to Data Importer requires Data Importer to create and/or maintain back doors and/or to facilitate access to Personal Data or systems with Personal Data, or require Data Importer to be in possession of, and/or to hand over, the encryption key to any third party (including, without limitation, law enforcement or other public authorities); (ii) Data Importer shall not facilitate access to Personal Data and/or systems with Personal Data to any governmental or local authorities or any other third party; and (iii) it has a special team and updated policies in place to deal with any kind of requests that involve disclosure of Personal Data to any governmental or local authorities or any other third party, and with the notification of such requests to the Data Exporter, policies to challenge disproportionate or unlawful requests, and policies to provide transparent information to data subjects about any disclosure of Personal Data to any governmental or local authorities or any other third party.

In case that Service Provider receives any request to disclose Personal Data, the Service Provider shall analyse the legality of any such order, the powers of the requesting party, and shall challenge and narrow the order to the maximum extent possible. When challenging an order, Service Provider shall seek interim measures to suspend the effects of the order until the court has finally decided on the merits. Service Provider shall not disclose the Personal Data requested until required to do so by the final decision of the competent court, and in such event, Service Provider hereby commits to provide only the minimum amount of information permissible.

12.1.3. In addition, where Company is established in Israel, it is hereby agreed that such transfer abroad, is made pursuant to Sections 2(4) and 3 of the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761-2001.

12.1.4. In the event that EU authorities or courts determine that the Restricted Transfer mechanism selected above is no longer an appropriate basis for Restricted Transfers, Company and the Service Provider shall promptly take all steps reasonably necessary to demonstrate adequate protection for the Company Personal Data, using another approved mechanism. Service Provider understands and agrees that Company may terminate the Restricted Transfers as needed to comply with the Data Protection Laws.

13. **INDEMNIFICATION**. Notwithstanding anything to the contrary in the Agreement or any agreement between the Parties, Service Provider shall indemnify, defend and hold harmless Company and each Company Affiliate against all losses, fines, penalties and sanctions arising from any claim of any kind by a Data Subject, third party or Supervisory Authority related to Personal Data, or arising from, or related to, any breach of this Addendum and/or violation of Data Protection law and/or a Personal Data Breach occurring in Service Provider's, Service Provider's Affiliates' and/or their Subprocessors' systems.

14. **LIABILITY**. Notwithstanding anything to the contrary in the Agreement or any agreement between the Parties, Service Provider's and Service Provider's Affiliates' liability related to Personal Data, or for any breach of, or related to, this Addendum, violation of Data Protection Law and/or Personal Data Breach occurring in Service Provider's, Service Provider's Affiliates' and/or their Subprocessors' systems shall be unlimited.

15. **CCPA**. Service Provider shall at all times: (i) comply with the CCPA and its regulations, including, without limitation, with respect to the Personal Data that Service Provider collects, receives, stores, or processes in accordance with this Addendum, providing the same level of privacy protections required of Company; (ii) forward to Company all consumer requests and cooperate with Company in accordance with Company's instructions with responding to, and complying with, consumer's requests; (iii) implement and maintain robust security procedures and practices to protect the Personal Data from unauthorized or illegal access, destruction, use, modification or disclosure; and (iv) conduct due diligence on its Subprocessors and have back to back contracts with each such Subprocessor that comply with the CCPA. Service Provider is prohibited from: (i) selling or sharing Company Personal Data (as the terms "sell" and "share" are defined under the CCPA); (ii) retaining, using, or disclosing the Company Personal Data for any purpose other than for the specific purpose of performing the Service, including retaining, using, or disclosing the Company Personal Data for a commercial purpose other than providing the Service; (iii) retaining, using, or disclosing the Company Personal Data outside of the direct business relationship between Service Provider and Company; or (iv) combining the Personal Data which the Service Provider receives from or on behalf of the Company, with Personal Data which it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer. Service Provider fully acknowledges and understands the above restrictions and will fully comply with them in an ongoing manner. Service Provider hereby agrees, understands and acknowledges that Service Provider does not receive from Company and Company does not pay Service Provider any monetary or other valuable consideration for Service Provider's collection of the Company Personal Data on behalf of Company.

16. MISCELLANEOUS

16.1 *Termination*

Subject to Section 16.2, the Parties agree that this Addendum and, if applicable, the Standard Contractual Clauses shall terminate automatically upon (i) termination of the Agreement; or (ii) expiry or termination of all service contracts, statements of work, work orders or similar contract documents entered into by Service Provider with Company and/or Company Affiliates pursuant to the Agreement, whichever is later.

Any obligation imposed on Service Provider under this Addendum in relation to the Processing of Personal Data shall survive any termination or expiration of this Addendum. Moreover, Section 13 and 14 and Company's remedies under law or equity in connection with any Processing of Company Personal Data, any breach of this Addendum and/or violation of Data Protection Law and/or a Personal Data Breach occurring in Service Provider's, Service Provider's Affiliates' and/or their Subprocessors' systems shall survive the termination of the Agreement, this Addendum and/or the Services for any reason.

16.2 *Governing law of this Addendum*

Without, if applicable, prejudice to Clause 9 (Governing Law) of the Standard Contractual Clauses, the governing law of this Addendum shall be the governing law stipulated in the Agreement.

16.3 *Choice of jurisdiction*

Without, if applicable, prejudice to Clause 7 (Mediation and Jurisdiction) of the Standard Contractual Clauses, and notwithstanding the choice of law under Section 16.3, the Parties to this Addendum hereby submit to the choice of

jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum. Notwithstanding the above, Company may seek interim relief before any court of competent jurisdiction worldwide.

16.4 *Breach*

Any breach of this Addendum shall constitute a material breach of the Agreement.

16.5 *Order of precedence*

With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the Parties, including but not limited to the Agreement, the provisions of this Addendum shall prevail with regard to the Parties' data protection obligations for Personal Data of a Data Subject from a Member State of the European Union. In the event of any conflict or inconsistency between this Addendum and the Clauses in Schedule 2 (*Standard Contractual Clauses*), if applicable, the Standard Contractual Clauses shall prevail. Notwithstanding anything to the contrary, this Addendum will supersede and prevail at all times over any Service Provider's online terms, pre-printed terms and conditions, including those contained in any purchase order, "click-through" agreements, other non-negotiated terms, confidentiality agreements, any similar agreement or any other business form submitted, or made available, by service provider to company name or its users before or after the effective date of this Addendum, including those made available as part of the platform or the Services, and/or on the Service Provider's website.

16.6 *Costs of compliance*

Each side will bear its own costs and expenses in order to ensure compliance with this Addendum and the Data Protection Laws requirements. Company and/or Company Affiliates shall not be obliged to pay any costs or expenses for Service Provider's and/or Service Provider's Affiliates' compliance with this Addendum.

16.7 *Third party rights*

Except to the extent set out in Section 16.9 and, if applicable, in Clause 3 of Schedule 2 (*Standard Contractual Clauses*), a person who is not a Party to this Addendum shall have no right to enforce any term of this Addendum.

A Company Affiliate may enforce any term of this Addendum which is expressly or implicitly intended to benefit it.

The rights of the Parties to rescind or vary this Addendum are not subject to the consent of any other person.

16.8 *Changes in Data Protection Laws*

Company may notify Service Provider in writing from time to time of any variations to this Addendum which are required as a result of a change in Data Protection Laws including without limitation to the generality of the foregoing, any variations which are (i) required and to the extent required as a result of any changes to the Data Protection Act 2018 following any exit of the UK from the European Union; (ii) update of the Standard Contractual Clauses by the European Commission, or (iii) required to take account of any new data transfer mechanisms for the purposes of Sections 12.1. Any such variations shall take effect on the date falling 30 (thirty) calendar days after the date such written notice is sent by Company and Service Provider shall procure that where necessary the terms in each contract between Service Provider or any Service Provider Affiliate and each Sub-processor are amended to incorporate such variations within the same time period.

16.9 *Severance*

Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

SCHEDULE 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Schedule 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing of the Company Personal Data are set out in the Agreement and this Addendum.

The nature and purpose of the transfers and processing of Company Personal Data

Service Provider is engaged to provide Services to Company which involve the Processing of Company Personal Data. The scope of the Services is set out in the Agreement, and the Company Personal Data will be Processed by the Service Provider and Service Provider Affiliates to deliver those Services and to comply with the terms of the Agreement and this Addendum.

The categories of Company Personal Data to be Processed (including, sensitive data) (insert description)

The Personal Data required for Service Provider to provide the Services as described in the Agreement. No sensitive data is included, except that the Parties agree otherwise in writing.

The categories of Data Subject to whom the Company Personal Data relates

Those individuals to whom the Personal Data relates. ***The obligations and rights of Service Provider and Service Provider Affiliates***

The obligations and rights of Service Provider and Service Provider Affiliates are set out in the Agreement and this Addendum.

The frequency of the transfer.

One-off or continuous basis, as applicable to provide the Services described in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As described in the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As described in Schedule 3.

SCHEDULE 2: STANDARD CONTRACTUAL CLAUSES

EU SCCs. Transfers to other countries. If the Processing of Personal Data includes transfers from the EEA to countries outside the EEA which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision, the Parties shall comply with Chapter V of the GDPR. The Parties hereby agree to execute the Standard Contractual Clauses as follows:

a) The Standard Contractual Clauses (EU Controller-to-Processor) and/or Standard Contractual Clauses (EU Processor-to-Processor) will apply (according to whether Company is a controller and/or processor) with respect to Restricted Transfers between Company and Service Provider that are subject to the EU GDPR.

b) The Parties agree that for the purpose of transfer of Personal Data between Company (as Data Exporter) and Service Provider (as Data Importer), the following shall apply: (i) Clause 7 of the Standard Contractual Clauses shall be not applicable; (ii) In Clause 9, option 1 (general written 1 (specific prior authorization) shall apply and the method that the data importer shall submit the request for appointing and time period for prior notice specific authorisation at least 30 days prior to the engagement of the sub-processor; (iii) In Clause 11, the optional language shall be applicable, and; (iv) In Clause 17, option 1 shall apply. The Parties agree that the Standard Contractual Clauses shall be governed by the laws of Ireland]; and (v) In Clause 18(b) the Parties choose the courts of Ireland, as their choice of forum and jurisdiction.

c) Annex I.A: With respect to Module Two: Data Exporter is Company as a data controller and the Data Importer is Service Provider as a data processor. With respect to Module Three: Data Exporter is Company as a data processor and the Data Importer is Service Provider as a data processor (sub-processor). Data Exporter and Data Importer Contact details: As detailed in the Agreement. Signature and Date: By entering into the Agreement and this Addendum, each Party is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of this Addendum.

d) Annex I.B of the Standard Contractual Clauses shall be completed as described in Schedule 1 (Details of the Processing of Company Personal Data) of this Addendum.

e) Annex I.C of the Standard Contractual Clauses shall be completed as follows: The competent supervisory authority is the Irish supervisory authority.

f) Annex II of the Standard Contractual Clauses shall be completed as described and agreed between the parties in the Agreement and/or this Addendum (including, Schedule 4 of this Addendum).

g) Annex III of the Standard Contractual Clauses shall be completed with the authorized sub-processors detailed in Schedule 3 (Authorised Sub-processors list) of this Addendum.

UK SCCs. If the Processing of Personal Data includes transfers from the UK to countries which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision, the Parties shall comply with Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018. The Parties hereby agree to execute the UK Standard Contractual Clauses as follows:

a) The UK Standard Contractual Clauses (UK Controller-to-Processor) and/or Standard Contractual Clauses (UK Processor-to-Processor) will apply (according to whether Company is a controller and/or processor) with respect to Restricted Transfers between Company and Service Provider that are subject to the UK GDPR.

b) The Parties agree that for the purpose of transfer of Personal Data between Company (as Data Exporter) and Service Provider (as Data Importer), the following shall apply: (i) Clause 7 of the Standard Contractual Clauses shall be not applicable; (ii) In Clause 9, option 1 (general written 1 (specific prior authorization)) shall apply and the method that the data importer shall submit the request for appointing and time period for prior notice specific authorisation at least 30 days prior to the engagement of the sub-processor; (iii) Clause 11 of the Standard Contractual Clauses shall be applicable; (iv) In Clause 17, option 1 shall apply. The Parties agree that the Standard Contractual Clauses shall be governed by the laws of England and Wales; and (v) In Clause 18(b) the Parties choose the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts, as their choice of forum and jurisdiction. Which Parties may end this Addendum as set out in Section 19: Importer and/or Exporter, in accordance with the agreed terms of this Addendum.

c) Annex I.A: With respect to Module Two: Data Exporter is Company as a data controller and the Data Importer is Service Provider as a data processor. With respect to Module Three: Data Exporter is Company as a data processor and the Data Importer is Service Provider as a data processor (sub-processor). Data Exporter and Data Importer Contact details: As detailed in the Agreement. Signature and Date: By entering into the Agreement and this Addendum, each Party is deemed to have signed these UK Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of this Addendum.

d) Annex I.B of the UK Standard Contractual Clauses shall be completed as described in Schedule 1 (Details of the Processing of Company Personal Data) of this Addendum.

e) Annex I.C of the UK Standard Contractual Clauses shall be completed as follows: The competent supervisory authority is the ICO supervisory authority.

f) Annex II of the UK Standard Contractual Clauses shall be completed as described and agreed between the parties in the Agreement and/or this Addendum.

g) Annex III of the UK Standard Contractual Clauses shall be completed with the authorized sub-processors detailed in Schedule 3 (Authorised Sub-processors list) of this Addendum.

SCHEDULE 3: AUTHORISED SUBPROCESSORS LIST

As notified by Service Provider in writing to Company 3 days after executing of the Agreement to ciso@growthspace.com with a copy to legal@growthspace.com

SCHEDULE 4: MIMIMUM SECURITY REQUIREMENTS

(applicable to Service Provider and Service Provider Affiliates)

1. Service Provider shall establish a procedure for allowing access to Company Personal Data and restriction of such access. Service Provider shall ensure that access to Company Personal Data is strictly limited to those individuals who "need to know" or need to access the relevant Company Personal Data and as strictly necessary for the purpose of providing the Services and shall keep record of the persons authorised to access the Company Personal Data.

2. Service Provider shall take all steps reasonably necessary to ensure the reliability of the individuals who may have access to Company Personal Data and shall ensure that each such individual (i) is informed of the confidential nature of Company Personal Data; (ii) has received appropriate training on his/her responsibilities; and (iii) is subject to written confidentiality undertakings and signs written security protocols.

3. To the extent required under Data Protection Law, Service Provider shall implement physical measures to ensure that access to the Company Personal Data is granted only to authorized users.

4. Service Provider shall maintain and implement sufficient and appropriate (based on the type of Company Personal Data and its sensitivity) environmental, physical and logical security measures with respect to Company Personal Data and to Service provider's system's infrastructure, data processing system (including the system in which the Company Personal Data is processed), communication means, terminals, system architecture, hardware and software, in order to prevent penetration and unauthorized

access to Company Personal Data or to the system or communication lines between Company and Service Provider. Service Provider further agrees that systems on which Company Personal Data is processed shall be located in a secure location, which may be accessed only by properly authorized employees.

5. The Service Provider shall maintain and store the Company Personal Data separately from any other data maintained by the Service Provider (whether such data is Service Provider's data or any third party data), and will ensure complete segregation between Company personal Data and any data held by Service Provider, as well as between the systems used by Service provider to provide Services to Company and its other systems, and between Service Provider's activity on behalf of Company, and its activity on behalf of other customers.

6. Service provider shall list all components (hardware and software) used to process Company Personal Data, including computer systems, communication equipment, and software. Service Provider shall use such list to continuously monitor such components and identify weaknesses and risks for the purpose of implementing appropriate security measures to mitigate them.

7. The Service Provider shall act in accordance with an appropriate security policy and working procedures that comply with the security requirements under this Annex and privacy laws, including with respect to backup and recovery procedures. Service Provider shall review its security policies and operating procedures periodically and not less than on an annual basis, and when material changes to the systems or processing are made, all in order to amend them, if required.

8. Service Provider shall take measures to record the access to the Company Personal Data, including recording the exit or entry of any employee for or into the facilities where the Company Personal Data is processed, as well as any equipment brought in or taken out of such facilities.

9. Service Provider shall implement automatic control mechanism for verifying access to systems containing Company Personal Data, which shall include, inter alia, the user identity, date and time of access attempt, the system component attempted to be accessed, type and scope of access and if access was granted or denied. Service Provider shall periodically monitor the information from the control mechanism, list issues and irregularities and the measures taken to handle them. Control records shall be maintained for a minimum of 24months. Service Provider records and any related reports and measures will be shared with Company, upon request, and to extent required under Data Protection Law, such records shall be backed-up by Service Provider.

10. Service Provider will perform security risk survey and penetration testing, at least once every 12 months and shall make required amendments in case of any irregularities are discovered. Service Provider records and any related reports and measures related to the risk survey and penetration testing will be shared with Company, upon request.

11. The Service Provider will not transfer Company Personal Data through a public communications network or via the internet, without using industry-standard encryption methods.

12. The Service Provider shall not allow use, copying or storage of Company Personal Data on personal or mobile devices.