**DATA PROCESSING ADDENDUM**

This Data Processing Addendum ("***DPA***") amends and forms part of the written agreement between **Customer** and HYCU, Inc. ("***HYCU***") (collectively, "***the parties***") for the provision of services to Customer (the "***Agreement***"). This DPA prevails over any conflicting term of the Agreement but does not otherwise modify the Agreement.

1. **Definitions**

1.1. In this DPA:

a) "**HYCU**" means HYCU, Inc., with its principal place of business at 27-43 Wormwood Street, Suite 650, Boston MA 02210, USA, or its affiliates as applicable. For clarity, unless otherwise stated in writing, the HYCU entity contracting with Customer hereunder will be (i) HYCU, Inc., if Customer is located in the United States or Canada; or (ii) HYCU Ltd., with its business address at 10 Earlsfort Terrace, Dublin 2, D02T380, Republic of Ireland, if Customer is located outside of the United States or Canada;

b) "***Controller***", "***Data Subject***", "***Processing***" (related terms such as "Process" and "Processed" shall have corresponding meanings), "***Processor***", "***Service Provider***", and "***Supervisory Authority***" have the meaning given to them in Data Protection Law (as defined below);

c) "***Data Protection Law***" means the General Data Protection Regulation (EU) 2016/679 ("***GDPR***") and all other Data Protection Laws of the European Union, the European Economic Area ("***EEA***"), and their respective Member States, Switzerland, and the United Kingdom ("***UK***"); (ii) certain U.S. federal and state privacy laws, including the California Consumer Privacy Act as amended by the California Privacy Rights Act (California Civil Code § 1798.100) ("***CCPA***"); and (iii) all laws implementing or supplementing the foregoing;

d) "***Data Subject Rights***" means all rights granted to Data Subjects by Data Protection Law, such as the right to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making;

e) "***Restricted Data Transfer***" means any international transfer of Personal Data that would be prohibited under Data Protection Law in the EEA or UK without implementation of additional safeguards such as Standard Contractual Clauses;

f) "***Personnel***" means any natural person acting under the authority of HYCU;

g) "***Personal Data***" means any information that constitutes "personal data" or "personal information" within the meaning of applicable Data Protection Law that HYCU Processes on behalf of Customer in performing the Services under the Agreement;

h) "***Personal Data Breach***" means the unauthorized destruction, loss, control, alteration, disclosure of, or access to, Personal Data for which HYCU is responsible. Personal Data Breaches do not include unsuccessful access attempts or attacks that do not compromise the confidentiality, integrity, or availability of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems;

i) "***Sell***" means to sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Personal Data to a third party for monetary or other valuable consideration;

j) "***Sensitive Data***" means any type of Personal Data that is designated as a sensitive or special category of Personal Data, or otherwise subject to additional restrictions under Data Protection Law or other laws to which the Controller is subject;

k) "***Services***" means the services and/or products to be provided by HYCU to Customer under the Agreement. The Services shall also include any required, usual, appropriate, or acceptable methods to perform activities related to the Services, including (a) carrying out the Services or the business of which the Services are a part, (b) carrying out any benefits, rights, and obligations related to the Services, (c) maintaining records relating to the Services, and (d) complying with any legal or self-regulatory obligations related to the Services;

l) "***Share***" means to share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Personal Data to third parties for targeted advertising to an individual based on Personal Data obtained from the individual's activity across non-affiliated or distinctly-branded websites, applications, or services;

m) "***Subprocessor***" means a Processor engaged by a Processor to carry out Processing on behalf of a Controller;

n) "***Standard Contractual Clauses***" means the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council as amended or replaced from time to time; and

o) **"*UK Addendum***" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner for parties making restricted transfers.

1.2. Capitalized terms used but not defined herein have the meaning given to them in the Agreement.

2. **Roles**

2.1. If Data Protection Law applies to the Processing of Personal Data, the parties agree that HYCU shall process Personal Data only as a (Sub)Processor acting on behalf of Customer and, with respect to CCPA and other applicable U.S. state privacy laws, as a Service Provider, in each case, regardless of whether Customer acts as a Controller or as a Processor on behalf of a third-party Controller with respect to Personal Data.

3. **Scope**

3.1. This DPA applies to Processing of Personal Data by HYCU in the context of the Agreement.

3.2. The subject matter, nature, and purpose of the Processing, the types of Personal Data, and categories of Data Subjects are set out in **Annex I**, which is an integral part of this DPA.

4. **Instructions**

4.1. HYCU will only Process Personal Data to provide the Services to Customer. Where Customer acts as a Processor on behalf of a third-party Controller, Customer warrants that Customer's instructions have been authorized by the relevant Controller.

4.2. It is the parties' intent that HYCU is a Service Provider, and HYCU certifies that it will not (a) Sell or Share Personal Data; (b) Process Personal Data outside the direct business relationship between the parties or for any purpose other than to provide the Services in accordance with the Agreement,

unless required or permitted by applicable laws; or (c) combine the Personal Data that HYCU receives from or on behalf of Customer with personal data that HYCU collects or receives from another person.

4.3. Customer's instructions are documented in **Annex I**, the Agreement, and any applicable statement of work.

4.4. Customer may issue additional instructions to HYCU as it deems necessary to comply with Data Protection Law. Such instructions must be provided to HYCU in writing and acknowledged in writing by HYCU as constituting instructions for purposes of this DPA, and HYCU may charge a reasonable fee to comply with any such additional instructions.

4.5. The parties acknowledge and agree that the disclosure of Personal Data by the Customer to HYCU does not form part of any monetary or other valuable consideration exchanged between the parties.

5. **Customer Responsibilities**

5.1 Customer is responsible for the lawfulness of Personal Data processing under or in connection with the Services. Customer shall (i) have provided, and will continue to provide all notices and have obtained, and will continue to obtain, all consents, permissions, and rights necessary under applicable Data Protection Law for HYCU to lawfully process Personal Data for the purposes contemplated by the Agreement (including this DPA); (ii) make appropriate use of the Services to ensure a level of security appropriate to the particular content of the Personal Data; (iii) have complied with all Data Protection Law applicable to the collection of Personal Data and the transfer of such Personal Data to HYCU and its Subprocessors; and (iv) ensure its processing instructions comply with applicable laws (including applicable Data Protection Law).

6. **Personnel and Subprocessing**

6.1. HYCU will take steps to ensure that all Personnel authorized to process Personal Data agree to appropriate confidentiality arrangements.

6.2. Customer authorizes HYCU to engage (including the disclosure of Personal Data under the Agreement to such Subprocessors): the Subprocessors included in the list of Subprocessors provided to Customer and set out in **Annex III** ("***Subprocessor List***"); and Subprocessors engaged in accordance with Section 6.3.

6.3. Where HYCU intends to engage any additional Subprocessor not already approved on the Subprocessor List, HYCU will notify Customer of the proposed engagement of the Subprocessor giving Customer the opportunity to object, and Customer may object only on reasonable grounds relating to a potential or actual violation of Data Protection Law. If Customer does not make a reasonable objection to the proposed engagement within 30 days of HYCU providing notice to Customer under this Section 6.3, Customer is deemed to have authorized the engagement of such Subprocessor. Where Customer raises a reasonable objection to the proposed engagement of a Subprocessor, HYCU may, at its discretion, make reasonable efforts to remedy the situation giving rise to the reasonable objection or propose an alternative Subprocessor to conduct the relevant Processing. In the event HYCU is unable to remedy the situation and no alternative Subprocessor is proposed, then HYCU will be entitled to terminate the Agreement without penalty or liability effective immediately on written notice to the Customer and the Customer shall pay HYCU any fees due for the Services performed prior to termination.

6.4. HYCU will enter into a written agreement with all Subprocessors which imposes substantially similar obligations on the Subprocessors as this DPA imposes on HYCU. HYCU will remain fully liable to the Customer for the performance of each Subprocessor's data protection obligations relating to this DPA in the event the Subprocessor fails to fulfil those obligations.

6.5. To the extent required by law, HYCU will provide a copy of HYCU's agreements with Subprocessors to Customer upon request. HYCU may redact commercially sensitive information before providing such agreements to Customer.

7. **Restricted Data Transfers**

7.1. Where Personal Data Processed under this DPA is subject to Data Protection Law in the EEA (and to the extent required by such law), by agreeing to this DPA Customer and HYCU conclude the Standard Contractual Clauses, which are hereby incorporated by reference. Where Customer is a Controller and HYCU is a Processor, the parties conclude Module 2 of the Standard Contractual Clauses. Where Customer is a Processor and HYCU is a Subprocessor, the parties conclude Module 3 of the Standard Contractual Clauses. The Standard Contractual Clauses are completed as follows: the "data exporter" is Customer; the "data importer" is HYCU; the optional docking clause in Clause 7 is implemented; Clause 9(a) option 2 is implemented and the time period therein is specified as thirty (30) days; the optional redress clause in Clause 11(a) is struck; Clause 13, (a) paragraph 2 is implemented; Clause 17 option 1 is implemented and the governing law is the law of the Republic of Ireland; the court in Clause 18(b) are the Courts of the Republic of Ireland; Annex 1 and 2 and 3 to module 2 of the Standard Contractual Clauses are **Annex I and II** to this DPA respectively.

7.2. Where Personal Data Processed under this DPA is subject to Data Protection Law in the UK (and to the extent required by such law), by signing this DPA Customer and HYCU agree to be bound by the UK Addendum which is hereby incorporated by reference and completed as follows: Part 1, table 1 of the UK Addendum will be deemed to be completed like its equivalent provisions in the Standard Contractual Clauses (module 2 or 3, as applicable) in Annex I, Section 1. For the purpose of Part 1, Table 2 of the UK Addendum, the Approved EU SCCs are the Standard Contractual Clauses (module 2 or 3, as applicable) incorporated by reference into this DPA pursuant to Section 7.1 of this DPA. For the purpose of Part 1, Table 3, Annex 1 and 2 to the Standard Contractual Clauses (module 2 or 3, as applicable) are **Annex I and II** to this DPA respectively. For the purpose of Part 1, Table 4, the party that may end the UK Addendum in accordance with Section 19 of the UK Addendum is the importer. Part 2, Mandatory Clauses of the UK Addendum shall be deemed completed with the following provision: "Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses".

8. **Security and Personal Data Breaches**

8.1. HYCU will implement and maintain appropriate technical and organizational measures in relation to the Processing of Personal Data designed to provide a level of security appropriate to the risks which may occur as a result of Processing Personal Data, and in particular the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, including the measures listed in **Annex II** (as appropriate).

8.2. HYCU will inform Customer without undue delay after becoming aware of a Personal Data Breach and provide Customer with details of the Personal Data Breach as required under Data Protection

Laws and reasonable assistance in remediating and mitigating the effects of the Personal Data Breach.

8.3. HYCU's notification of or response to a Personal Data Breach under Section 8.2 will not be construed as an acknowledgement by HYCU of any fault or liability with respect to the Personal Data Breach.

8.4. In the event of a Personal Data Breach, Customer is solely responsible for determining whether Data Protection Law requires the notification of affected individuals, regulators, and other parties.

9. **Assistance**

9.1. HYCU will reasonably assist Customer, including by implementing appropriate technical and organizational measures, with the fulfilment of Customer's own obligations under Data Protection Law, including:

a) complying with Data Subjects' requests to exercise Data Subject Rights;

b) replying to inquiries or complaints from Data Subjects;

c) replying to investigations and inquiries from Supervisory Authorities;

d) conducting data protection impact assessments, and prior consultations with Supervisory Authorities; and

e) notifying Personal Data Breaches.

9.2. Unless prohibited by Data Protection Law, HYCU will inform Customer as soon as reasonably practicable if HYCU:

a) receives a request, complaint, or other inquiry regarding the Processing of Personal Data from a Data Subject or Supervisory Authority;

b) receives a binding or non-binding request to disclose Personal Data from law enforcement, courts or any government body;

c) is subject to a legal obligation that requires HYCU to Process Personal Data in contravention of Customer's instructions; or

d) is otherwise unable to comply with Data Protection Law or this DPA.

9.3. Unless prohibited by Data Protection Law, HYCU will obtain Customer's written authorization before responding to, or complying with any requests, orders, or legal obligations referred to in Section 9.2.

10. **Accountability**

10.1. Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate HYCU's unauthorized use of Personal Data.

10.2. HYCU will inform Customer without undue delay if HYCU believes that a written instruction by Customer, pursuant to this DPA, violates Data Protection Law, in which case HYCU may suspend the Processing until Customer has modified or confirmed the lawfulness of the instructions in writing.

11. **Audit**

11.1. Upon Customer's prior written request, and no more than once in a calendar year, HYCU will make available to Customer the required information reasonably necessary to demonstrate compliance with the obligations of Data Protection Law and this DPA. HYCU shall provide additional information

as reasonably necessary to allow for and contribute to audits, including inspections, conducted by a Supervisory Authority, Customer, or another auditor mandated by law.

11.2. If a third party is to conduct a Customer-requested audit, HYCU may object to the auditor if the auditor is, in HYCU's reasonable opinion, not suitably qualified or independent, a competitor of HYCU, or otherwise manifestly unsuitable. Such objection by HYCU will require Customer to appoint another auditor or conduct the audit itself.

11.3. The audit must be conducted during regular business hours at the applicable facility, subject to an audit plan agreed to between the parties at least two weeks in advance and may not unreasonably interfere with HYCU's business activities.

11.4. If Customer's requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST, or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request and HYCU confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

11.5. Any Customer-requested audits are at Customer's expense. Customer shall reimburse HYCU for any time expended by HYCU or its Subprocessors in connection with any Customer-requested audits or inspections at HYCU's then-current professional services rates, which shall be made available to Customer upon request.

11.6. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports are confidential information of the parties under the terms of the Agreement.

12. **Liability**

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

13. **Confidentiality**

13.1. HYCU will keep all Personal Data and all information relating to the Processing thereof, in strict confidence.

14. **Analytics**

15.1 Customer acknowledges and agrees that HYCU may create and derive from Processing related to the Services anonymized and/or aggregated data that does not identify Customer or any natural person, and use, publicize, or share with third parties such data to improve HYCU's products and services and for its other legitimate business purposes.

15. **Notifications**

15.1. HYCU will make all notifications required under this DPA as agreed to in the Agreement or the established daily point of contact with the Customer.

16. **Term and Duration of Processing**

16.1. On expiration or termination of the Agreement, or upon written request from Customer at any time, HYCU will, as soon as reasonably practicable, return or securely delete and destroy all Personal Data in HYCU's possession or control, except as otherwise required by law or set out in

the Agreement. Upon request from Customer, HYCU will certify such secure deletion in writing within thirty (30) days of Customer's request.

17. **Modification of this DPA**

17.1. This DPA may only be modified by a written amendment signed by both Customer and HYCU.

18. **Invalidity and Severability**

18.1. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

**ANNEX I**

**A. LIST OF PARTIES**

Customer is the data exporter and HYCU is the data importer.

**B. DESCRIPTION OF TRANSFER**

| | |
|---|---|
| **Subject Matter** | HYCU's provision of backup and recovery services to Customer. |
| **Duration of the Processing** | For the term of the Agreement and as required under applicable law. |
| **Nature and Purpose of the Processing** | HYCU will process Personal Data for the purposes of providing the Services to Customer in accordance with the DPA. |
| **Frequency of the Processing** | Continuous. |
| **Categories of Data** | Data relating to individuals provided to HYCU in connection with the Services, by or at the direction of Customer. |
| **Sensitive Data Processed** | The Services are not intended to Process Sensitive Data unless otherwise agreed to in a signed amendment to this Annex. |
| **Data Subjects** | Customer's end users and employees. |

**C. COMPETENT SUPERVISORY AUTHORITY**

The competent supervisory authority is the Irish Data Protection Commission.

## ANNEX II

HYCU shall implement and maintain the controls listed in this Annex II in accordance with industry standards generally accepted by information security professionals as necessary to reasonably protect Personal Data during storage, processing, and transmission.

**Physical access control**

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers, and related hardware), where Personal Data is Processed, include: (a) establishing security areas, restriction of access paths; (b) establishing access authorizations for employees and third parties; (c) access control system (ID reader, magnetic card, chip card); (d) key management, card-keys procedures; (e) door locking (electric door openers, etc.); (f) security staff, janitors; (g) surveillance facilities, video/CCTV monitor, alarm system; and (h) securing decentralized data processing equipment and personal computers.

**Virtual access control**

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include: (a) user identification and authentication procedures; (b) ID/password security procedures (special characters, minimum length, change of password); (c) automatic blocking (e.g., password or timeout); (d) monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts; (e) creation of one master record per user, user-master data procedures per data Processing environment; and (f) encryption of archived data media.

**Data access control**

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified, or deleted without authorization, include: (a) internal policies and procedures; (b) control authorization schemes; (c) differentiated access rights (profiles, roles, transactions and objects); (d) monitoring and logging of accesses; (e) disciplinary action against employees who access Personal Data without authorization; (f) reports of access; (g) access procedure; (h) change procedure; (i) deletion procedure; and (j) encryption.

**Disclosure control**

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport, or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include: (a) encryption/tunneling; (b) dynamic data masking; (c) logging; and (d) transport security.

**Entry control**

Technical and organizational measures to monitor whether Personal Data has been entered, changed, or removed (deleted), and by whom, from data processing systems, include: (a) logging and reporting systems; and (b) audit trails and documentation.

**Availability control**

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include: (a) backup procedures; (b) mirroring of hard disks (e.g., RAID technology); (c) uninterruptible power supply (UPS); (d) remote storage; (e) antivirus/firewall systems; and (f) disaster recovery plan.

**Separation control**

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include: (a) separation of databases; (b) "internal client" concept / limitation of use; (c) segregation of functions (production/testing); and (d) procedures for storage, amendment, deletion, transmission of data for different purposes.

**ANNEX III**

**List of Subprocessors**

Customer authorizes HYCU to engage the following Subprocessors:

| **Subprocessor Company Name** | **Subprocessor Location** | **(Description of Processing activities carried out by Subprocessor)** |
|---|---|---|
| Google (as provider of Google Cloud Platform) | EU or US at customers designation | Hosting & IaaS provider for backing up data on Google, SaaS/DBaaS/PaaS services and for spinning up non-GCP native workloads on Google Cloud |
| Amazon Web Services | EU or US at customers designation | Hosting & IaaS provider for backing up data on AWS, SaaS/DBaaS/PaaS services and for spinning up non-AWS native workloads on AWS |
| Microsoft Corporation (as provider of Azure) | EU or US at customers designation | Hosting & IaaS provider for backing up data on Azure, and for spinning up non-Azure native workloads on Azure |
| DropSuite International | US, UK, Canada, EU, Singapore, Japan, or Australia at customer designation | Infrastructure for Microsoft M365 and Google Workspace backup |
| Zendesk | US | Support ticket management |
| AskNicely | US, EU | To continuously assess the customer's experience with HYCU |