DATA PROCESSING AGREEMENT

This Data Processing Agreement (**DPA**) is made between Beany UK Limited, a company registered in England and Wales with company number 13961812 (**we**, **us** or **our**) and you, the individual or entity that is entered into the Beany UK Terms and Conditions (**Terms and Conditions**) with us (**you** or **your**), together the **Parties** and each a **Party**. This DPA is incorporated into, and supplements the Terms and Conditions.

Background

A. The Parties have entered into the Terms and Conditions for the provision of Services.

B. In the processing of Customer Personal Data in connection with the Terms and Conditions, each Party will perform the role/s set out in Annex 1 Part A.

C. The Parties would like to implement this DPA to set out each Party's rights and obligations in connection with the Processing of Customer Personal Data under the Terms and Conditions.

1. Commencement and Term

This DPA will commence on the date it is executed between the Parties and will continue for as long as the Terms and Conditions remain in effect, or the Processor retains any of the Customer Personal Data in its possession or control (whichever is the longer) (**Term**).

2. Processing of Personal Data

2.1 The Processor agrees to:

(a) comply with all Applicable Data Protection Laws in the Processing of Customer Personal Data; and

(b) not process Customer Personal Data other than on the Controller's documented instructions.

2.2 The Controller instructs the Processor to process Personal Data in accordance with this DPA (including in accordance with Annex 1).

2.3 You agree to inform us without undue delay if you are not able to comply with your responsibilities under this clause 3 or Applicable Data Protection Laws.

3. Processor Personnel

3.1 The Processor agrees to take reasonable steps to ensure the reliability of any of the Contracted Processor's Personnel who may have access to the Customer Personal Data, ensuring in each case that:

(a) access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Terms and Conditions; and

(b) The relevant Personnel are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 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, the Processor agrees to implement appropriate technical and organisational measures in relation to the Customer Personal Data to ensure a level of security appropriate to that risk in accordance with Applicable Data Protection Laws, and as further particularised in Annex 2.

4.2 In assessing the appropriate level of security, the Processor agrees to take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub-Processing

5.1 The Controller authorises the Processor's engagement of the Sub-Processors already engaged by the Processor at the date of this DPA that are set out in Annex 2.

5.2 Where the Processor wishes to engage a new Sub-Processor, the Processor agrees to provide written notice to the Controller of the details of the engagement of the Sub-Processor at least 14 days' prior to engaging the new Sub-Processor (including details of the processing it will perform). The Controller may object in writing to the Processor's appointment of a new Sub-Processor within 7 days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the Parties will discuss such concerns in good faith with a view to achieving resolution. If the Parties are not able to achieve resolution, the Processor may, at its election:

(a) not appoint the proposed Sub-Processor;

(b) not disclose any Customer Personal Data it processes on the Controller's behalf to the proposed Sub-Processor; or

(c) inform the Controller that it may terminate the Terms and Conditions (including this DPA) for convenience, in which case, clause 13.2 will apply.

5.3 The Controller agrees that the remedies described above in clauses 5.2(a)-(c) are the only remedies available to the Controller if it objects to any proposed Sub-Processor by the Processor.

5.4 Where the Processor engages a Sub-Processor to process Customer Personal Data, the Processor agrees to:

(a) enter into a written agreement with the Sub-Processor containing data protection obligations no less protective that those in this DPA with respect to the Customer Personal Data; and

(b) remain responsible to the Controller for the performance of such Sub-Processor's data protection obligations under such terms

(c) where the transfer of Customer Personal Data to a Sub-Processor is a Restricted Transfer, ensure that such written agreement contains the SCCs in order to provide adequate safeguards for the transfer of such Customer Personal Data in accordance with applicable Data Protection Laws.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, the Processor agrees to assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligations, as reasonably understood by the Controller, to respond to requests to exercise Data Subject rights under the Applicable Data Protection Laws.

6.2 The Processor agrees to:

(a) promptly notify the Controller if it receives a request from a Data Subject under any Applicable Data Protection Law in respect of Customer Personal Data; and

(b) ensure that it does not respond to that request except on the documented instructions of the Controller or as required by Applicable Data Protection Laws to which the Processor is subject, in which case the Processor shall, to the extent permitted by Applicable Data Protection Laws, inform the Controller of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 The Processor agrees to notify the Controller without undue delay upon the Processor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing the Controller with sufficient information to allow the Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 The Processor agrees to cooperate with the Controller and take reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.3 If the Controller decides to notify a Supervisory Authority, Data Subjects or the public of a Customer Personal Data Breach, the Controller agrees to provide the Processor with advance copies of the proposed notices and, subject to Applicable Data Protection Law (including any mandated deadlines under the GDPR), allow the Processor an opportunity to provide any clarifications or corrections to those notices.

8. Data Protection Impact Assessment and Prior Consultation

The Processor agrees to provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law (to the extent the Controller does not otherwise have access to the relevant information and such information is in the Processor's control).

9. Deletion or return of Personal Data

9.1 Subject to this clause 9, and subject to any document retention requirements at law, the Processor agrees to promptly and in any event within [10 business days] of the date of cessation of any Services involving the Processing of Customer Personal Data (**Cessation Date**), delete and procure the deletion of all copies of those Customer Personal Data.

10. Audit Rights

10.1 Subject to this clause 10, where required by law, the Processor shall make available to the Controller on request all information reasonably necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by the Controller or an auditor mandated by the Controller in relation to the Processing of the Customer Personal Data by the Contracted Processors.

10.2 Where clause 10.1 applies, any audit (or inspection):

(a) must be conducted during the Processor's regular business hours, with reasonable advance notice (which shall not be less than 30 business days);

(b) will be subject to the Processor's reasonable confidentiality procedures;

(c) must be limited in scope to matters specific to the Controller and agreed in advance with the Processor;

(d) must not require the Processor to disclose to the Controller any information that could cause the Processor to breach any of its obligations under Applicable Data Protection Laws;

(e) to the extent the Processor needs to expend time to assist the Controller with the audit (or inspection), will be funded by the Controller, in accordance with pre-agreed rates; and

(f) may only be requested by the Controller a maximum of one time per year, except where required by a competent Supervisory Authority or where there has been a Personal Data Breach in relation to Customer Personal Data, caused by the Processor.

10.3 Information and audit rights of the Controller only arise under section 10.1 to the extent that the Terms and Conditions does not otherwise give it information and audit rights meeting the relevant requirements of Applicable Data Protection Law.

11. Liability

Despite anything to the contrary in the Terms and Conditions or this DPA, to the maximum extent permitted by law, the Liability of each Party and its affiliates under this DPA is subject to the exclusions and limitations of Liability set out in the Terms and Conditions

12. Termination

12.1 Each Party agrees that a failure or inability to comply with the terms of this DPA and/or the Applicable Data Protection Laws constitutes a material breach of the Terms and Conditions. In such event, the Controller may, without penalty:

(a) require the Processor to suspend processing of Customer Personal Data until such compliance is restored; or

(b) terminate the Terms and Conditions effective immediately on written notice to the Processor.

12.2 In the case of such suspension or termination, the Processor shall provide a prompt pro-rata refund of all sums paid in advance under the Terms and Conditions which relate to the period of suspension or the period after the date of termination (as applicable).

12.3 Notwithstanding the expiry or termination of this DPA, this DPA will remain in effect until, and will terminate automatically upon, deletion by the Processor of all Customer Personal Data covered by this DPA, in accordance with this DPA.

13. General

13.1 **Amendment:** Other than as expressly permitted under this DPA and to the extent permitted by law, this DPA may only be amended by written instrument executed by the Parties.

13.2 **Assignment**: A Party must not assign or deal with the whole or any part of its rights or obligations under this DPA without the prior written consent of the other Party (such consent not to be unreasonably withheld).

13.3 **Confidentiality**: Each Party agrees to keep this DPA and any information it receives about the other Party and its business in connection with this DPA (**Confidential Information**) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law; or

(b) the relevant information is already in the public domain.

13.4 **Contracts (Rights of Third Parties) Act 1999:** Notwithstanding any other provision of this DPA, nothing in this DPA confers or is intended to confer any right to enforce any of its terms on any person who is not a party to it.

13.5 **Counterparts:** This DPA may be executed in any number of counterparts that together will form one instrument.

13.6 **Order of Precedence:** In the event of any conflict or inconsistency between the agreements entered into between the Parties, the SCCs shall prevail, then the Annexes, followed by this DPA and then the Terms and Conditions.

13.7 **Governing law and disputes:** This DPA is governed by the laws of England and Wales. Each Party irrevocably and unconditionally submits to the exclusive jurisdiction of the courts operating in England and Wales and any courts entitled to hear appeals from those courts and waives any right to object to proceedings being brought in those courts.

13.8 **Notices:** Any notice given under this DPA must be in writing addressed to the relevant address last notified by the recipient to the Parties. Any notice may be sent by standard post or email, and will be deemed to have been served on the expiry of 48 hours in the case of post, or at the time of transmission in the case of transmission by email.

13.9 **Severance:** If a provision of this DPA is held to be void, invalid, illegal or unenforceable, that provision is to be read down as narrowly as necessary to allow it to be valid or enforceable, failing which, that provision (or that part of that provision) will be severed from this DPA without affecting the validity or enforceability of the remainder of that provision or the other provisions in this DPA.

14. Definitions and Interpretation

14.1 In this DPA, unless the context otherwise requires, all terms have the meanings given to them in the Appendices and Annexures, and:

Applicable Data Protection Law means the laws and regulations applicable to the processing of Personal Data by the Parties in connection with the Terms and Conditions, including the UK GDPR.

Customer Personal Data means any Personal Data Processed by a Contracted Processor on behalf of a Controller in connection with the Terms and Conditions (and where the Processor is also acting as a Controller, any Personal Data it processes in connection with the Terms and Conditions).

Contracted Processor means the Processor or a Sub-Processor.

Controller means the Party specified in the Party Details of Annex 1 as the Controller that performs the role of a Controller as that term is defined under the UK GDPR.

Data Subject means any individual person that is identified or identifiable by way of Personal Data.

DPA means this Data Processing Agreement and all Annexes attached to it.

EU GDPR means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

Liability means any expense, cost, liability, loss, damage, claim, notice, entitlement, investigation, demand, proceeding or judgement (whether under statute, contract, equity, tort (including negligence), misrepresentation, restitution, indemnity or otherwise), howsoever arising, whether direct or indirect and/or whether present, unascertained, future or contingent and whether involving a third party or a Party to this DPA or otherwise.

Personnel means in respect of a Contracted Processor, any of its employees, consultants, and subcontractors.

Processor means the Party specified in the Party Details in Annex 1 as a Processor that performs the role of a Processor as that term is defined under the UK GDPR.

Restricted Transfer means a transfer of personal data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

SCCs means the standard data protection clauses for processors adopted pursuant to or permitted under Article 46 of the UK GDPR, as may be amended, superseded or replaced from time to time.

Services means the services subject to the Terms and Conditions.

Sub-Processor means any person appointed by or on behalf of the Processor to process Customer Personal Data on behalf of the Controller in connection with the Terms and Conditions.

UK GDPR means the Data Protection Act 2018 and the EU GDPR as incorporated into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.

14.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the UK GDPR.

14.3 The terms, "Data Exporter" and "Data Importer" shall have the same meaning as in the SCCs.

14.4 The word include shall be construed to mean include without limitation.

ANNEX 1

PART A: LIST OF PARTIES

we, us or our	**Beany UK Limited, a company registered in England and Wales with company number 13961812.** **Address:** 71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ **Phone:** 0808 164 3905 **Email:** support@beany.uk **Key Contact Key contact person's contact details and role:** Charlotte Wass, UK General Manager, charlotte@beany.com **Role:** Where you provide personal data to us to sign up to our Services, we are acting as a Controller. Where you input personal data into the Services and we process it on your behalf, we are acting as a Processor. Where we are acting as you Processor, you are the Controller.
you or your	**Name:** The individual or entity identified in the Terms and Conditions as our customer. **Address:** Your address as specified when signing up to our Services. **Phone:** Your contact number as specified when signing up to our Services. **Email:** Your email address as specified when signing up to our Services. **Key Contact Key contact person's contact details and role:** As specified when signing up to our Services. **Role:** Where you provide personal data to us to sign up to our Services, we are acting as a Controller. Where you input personal data into the Services and we process it on your behalf, we are acting as your Processor and you are the Controller.

PART B: DESCRIPTION OF TRANSFER

Personal Data Transferred	• Identity Data including first name, last name, date of birth, gender, salary and job title. • Contact Data of you and your staff (including their staff including staff addresses, email addresses and telephone numbers). • Employee details including Identity Data and Contact Data of past, present and future employees. • Financial Data including bank account and payment card details. • Third Party Product data, including data from any third party product, such as Xero, that you link to your Beany account. • Background Verification Data including, a photo identification document such as passport or Drivers' Licence, national insurance number and Unique Tax References (UTRs) to comply with due diligence obligations, anti-money laundering laws and related ongoing monitoring commitments. • Technical and Usage Data including internet protocol (IP) address, login data, browser session and geo-location data, device and network information, statistics on page views and sessions, acquisition sources, search queries and/or browsing behaviour, information about user access and use of our website, including through the use of Internet cookies, communications with our website, the type of browser used by users, the type of operating system used by users and the domain name of users' Internet service provider. • Profile Data including usernames and passwords for our platform, purchases or orders made with us, support requests made with us, content shared through our platform. • Marketing and Communications Data including preferences in receiving marketing from us and our third parties and communication preferences.
Special Categories of Personal Data and criminal convictions and offences	We do not actively collect special categories of data however we may come across information about criminal convictions and offences when undertaking our "Proof of Identity Checks".
Relevant Data Subjects	• Authorised users of the Services. • Anyone about whom personal data is input into the Service (including where it is imported from a third party product). • Your key business representatives that sign up to our Services, and where we are conducting "Proof of Identity Checks".
Frequency of the transfer	Continuous
Nature of the transfer	As specified in the Terms and Conditions, this DPA and as instructed by you, including without limitation: • use by us of Customer Personal Data to provide the Services; • collection, organisation, storage (hosting), retrieval and other processing of Customer Personal Data by us necessary to provide, maintain and improve the Services; and • transmission, disclosure and dissemination of Customer Personal Data to provide the Services in accordance with the Terms and Conditions or as compelled by law.
Purpose of processing	The purpose of the transfer and processing are as specified in the Terms and Conditions and this DPA.
Duration of the Processing	The term of the Terms and Conditions and for a period of 30 days after termination or expiry of the Terms and Conditions, except where required by law.

PART C: COMPETENT SUPERVISORY AUTHORITY

Information Commissioner's Office (in the UK)

ANNEX 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

TECHNICAL AND ORGANISATIONAL MEASURES	DETAILS
Designated data protection officer	• John Curtis (Chief Technology Officer, Beany)
Internal policies e.g. security policy, data retention and deletion policies	• All active customer data shall be retained for as long as the customer continues to be an active customer of Beany or unless the active customer has requested the deletion of data.
Pseudonymisation and encryption of personal data	• All customer data is encrypted in transit (using industry standard HTTPS or SSL protocols). • Data at rest is encrypted with PGP encryption
Product security features	• Your Beany account can be protected with multi-factor authentication. • We support SSO logins from Xero for convenience and security
Network security	• Beany's infrastructure including production and test environments, firewalls and network is hosted on Google Cloud (GCP) based in London. A description of Google Cloud's security is here. • Our security is tested for network security (penetration test) on each software release • Auditing / logging of all interactions with our software platform is done at several levels in our infrastructure from application logs to network access.
Physical security and disaster recovery	• Beany UK Ltd has no offices and does not accept paperwork. • All documentation is stored in our cloud environment. • Client documentation is worked on in a cloud environment and does not persist on staff devices. • No physical security on office premises is required • Full backups of client documents and data exist only in encrypted cloud storage.
Human resources security	• Auditing / logging of all interactions with our software platform is done at several levels in our infrastructure from application logs to network access. • Appropriate background checks are conducted on all employees in accordance with documented policies. • Business obtains written commitment of employees and contractors to maintain confidentiality in employment contracts and contractors agreements.

	● Access is revoked on a timely basis in accordance with security procedures upon the departure of any personnel. ● Information security awareness training is provided to all employees during onboarding and revised annually.

ANNEX 3

LIST OF SUBPROCESSORS

- Connect
- Hubspot
- Mailchimp
- Google
- Zendesk