Data Processing Agreement

The Terms of this Data Processing Agreement apply to and are binding on the Parties where Billy Inc. (Billy) acts as a data processor on your behalf and you act as data controller for the purposes of the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")

1. **Agreed terms**

The terms and expressions set out in this Agreement shall have the following meanings:

1.1. **Data Protection Legislation**: (i) unless and until the GDPR is no longer directly applicable, the General Data Protection Regulation (*(EU) 2016/679*), as amended or updated from time to time, (i) then (ii) any successor legislation to the GDPR;
1.2. **"Controller", "Processor", "Processing" and "Data Subject"** shall have the meanings given to them in the Data Protection Legislation;
1.3 **ICO** means the Information Commissioner's Office;
1.4 **Personal Data** means all such "personal data" as defined in the Data Protection Legislation as is, or is to be, processed by the Processor on behalf of the Controller;
1.5 **Services** means those services described in Schedule 1 which are provided by the Processor to the Controller and which the Controller uses for the purpose described in Schedule 1.

1.6 "Security Measures" means the security measures set out in Schedule 2

1.7 Clause, Schedule and paragraph headings shall not affect the interpretation of this agreement.

1.8 A **person** includes a natural person, corporate or unincorporated body (whether or not having separate legal personality).

1.9 The Schedules form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.

1.10 A reference to a **company** shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.11 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

1.12 Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.

It Is Agreed as follows:

2. Scope of Processing

2.1 The Controller determines the purposes and means of the processing of Personal Data. The Controller shall comply with its obligations pursuant to Data Protection Legislation, including responsibility to ensure necessary legal basis for collecting, processing and transfer of Personal Data.

2.2 The terms of this Agreement supersede any other arrangement, understanding or agreement made between the Parties at any time relating to protection of Personal Data.

2.3 This Agreement concerns the Processor's processing of Personal Data on behalf of the Controller in connection with the Processor's provision of the Services or otherwise as described in Schedule 1.

2.4 The Processor, its Sub-processors, and other persons acting under the authority of the Processor who has access to the Personal Data shall process the Personal Data only on behalf of the Controller and in compliance with its documented instructions and in accordance with the Processing Agreement, unless otherwise stipulated in applicable statutory laws.

2.5 The Processor shall immediately inform the Controller if, in the Processor's opinion, an instruction infringes the Data Protection Legislation.

2.6 The Processor shall promptly comply with any request from the Controller requiring the Processor to amend, transfer or delete the Personal Data.

2.7 The Processor agrees to comply with any reasonable measures required by the Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with the Data Protection Legislation and all applicable legislation from time to time in force and any best practice guidance issued by the ICO.

2.8 Where the Processor processes Personal Data (whether stored in the form of physical or electronic records) on behalf of the Controller it shall:

2.8.1 process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations to the Controller or as is required by law or any regulatory body including but not limited to the ICO;

2.8.2 implement appropriate technical and organisational measures and take all steps necessary to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, and promptly supply details of such measures as requested from the Controller;

2.8.3 any transfer of Personal Data is subject to the Data Protection Legislation's standard contractual clauses or other legal basis for such transfer or disclosure; and

2.8.4 if so requested by the Controller (and within the timescales required by the Controller) supply details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access.

2.9 The Processor shall notify the Controller (within two working days) if it receives:

2.9.1 a request from a data subject to have access to that person's Personal Data; or

2.9.2 a complaint or request relating to the Controller's obligations under the Data Protection Legislation.

2.10 The Processor agrees to provide the Controller with full co-operation and assistance in relation to any complaint or request made, including by:

2.10.1 providing the Controller with full details of the complaint or request;

2.10.2 complying with a data access request within the relevant timescale and in accordance with the Controller's instructions;

2.10.3 providing the Controller with any Personal Data it holds in relation to a data subject (within the timescales required by the Controller);

2.10.4 providing the Controller with any information requested by the Controller;

2.10.5 notify the Controller immediately if it becomes aware of any unauthorised or unlawful processing, loss of, damage to or destruction of any of the Personal Data.

3. Security Measures

3.1 The Processor shall implement appropriate technical and organisational measures as stipulated in Data Protection Legislation and/or measures imposed by the ICO to ensure an appropriate level of security and these are outlined in Schedule 2.

3.2 The Processor shall assess the appropriate level of security and take into account the risks related to the processing, including risk for accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Person Data transmitted, stored or otherwise processed.

3.3 All transmissions of Personal Data between the Processor and the Controller or between the Processor and any third party shall be done by means of adequate encryption.

3.4 The Processor shall provide the Controller with general descriptions of the Processor's and its Sub-processors' (to the extent that the Processor has access to such Sub-processors information) technical and organisational measures implemented to ensure an appropriate level of security.

3.5 The Processor shall provide reasonable assistance to the Controller, taking into account relevant information available to the Processor, if the Controller is obliged to perform an impact assessment and/or consult ICO in connection with the processing of Personal Data. The Controller shall bear any costs accrued by the Processor related to such assistance.

4. Notification of any Breach

4.1 The Processor shall notify the Controller without undue delay after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed ("**Personal Data Breach**"). The Controller is responsible for notifying the Personal Data Breach to the ICO within 72 hours of any such breach.

4.2 The notification to the Controller shall as a minimum describe (i) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) the likely consequences, in the reasonable opinion of the Processor, of the Personal Data Breach; (iii) the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.3 In the event the Controller is obliged to communicate a Personal Data Breach to the Data Subjects, the Processor shall assist the Controller, including the provision, if available, of necessary contact information to the affected Data Subjects. The Controller shall bear any costs related to such assistance provided by the Processor and to such communication to the Data Subject. The Processor shall nevertheless bear such costs if the Personal Data Breach is caused by circumstances for which the Processor is responsible.

5. Confidentiality

5.1 The Processor shall maintain the Personal Data processed by the Processor on behalf of the Controller in confidence, and in particular, unless the Controller has given written consent for the Processor to do so, the Processor shall not disclose any Personal Data supplied to the Processor by, for, or on behalf of, the Controller to any third party. The Processor shall not process or make any use of any Personal Data supplied to it by the Controller otherwise than in connection with the provision of the Services to the Controller.

5.2 The Controller is subject to a duty of confidentiality regarding any documentation and information, received by the Processor, related to the Processor's and its Sub-processors' implemented technical and organisational security measures.

5.3 The obligations in this Clause 7 shall continue for a period of five years after the cessation of the provision of Services by the Processor to the Controller. Nothing in this Agreement shall prevent either party from complying with any legal obligation imposed by the ICO or a court. Both parties shall however, where possible, discuss together the appropriate response to any request from the ICO or court for disclosure of information.

6. Term and Termination

6.1 The Processing Agreement is valid for as long as the Processor processes Personal Data on behalf of the Controller.
6.2 In the event of the Processor's breach of the Processing Agreement, the Controller may (i) instruct the Processor to stop further processing of Personal Data with immediate effect; (ii) terminate the Processing Agreement with immediate effect.
6.3 The Processor shall, upon the termination of this Agreement and at the choice of the Controller, delete or return all the Personal Data to the Controller, unless otherwise stipulated otherwise in the Data Protection Legislation. The Processor shall document in writing to the Controller that deletion has taken place.

Schedule 1 – Services

The "Services" means provision of Billy Accounting Software.

The Controller uses the Services for the purpose of providing bookkeeping, invoicing and accounting services online.

Schedule 2 – Security Measures

Security Measures referrs to:

1. The Processor will ensure that in respect of all Personal Data it receives from or processes on behalf of the Controller it maintains security measures to a standard appropriate to:

1.1 the harm that might result from unlawful or unauthorised processing or accidental loss, damage or destruction of the Personal Data; and

1.2 the nature of the Personal Data.

2. In particular the Processor shall:

2.1 have in place and comply with a security policy which:

2.1.1 defines security needs based on a risk assessment;

2.1.2 allocates responsibility for implementing the policy to a specific individual or members of a team;

2.1.3 is disseminated to all relevant staff; and

2.1.4 provides a mechanism for feedback and review.

2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;

2.3 prevent unauthorised access to the Personal Data;

2.4 ensure its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

2.5 have secure methods in place for the transfer of Personal Data whether in physical form (for instance, by using couriers rather than post) or electronic form (for instance, by using encryption);

2.6 put password protection on computer systems on which Personal Data is stored and ensure that only authorised personnel are given details of the password;

2.7 take reasonable steps to ensure the reliability of employees or other individuals who have access to the Personal Data;

2.8 ensure that any employees or other individuals required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this Agreement;

2.9 ensure that none of the employees or other individuals who have access to the Personal Data publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller;

2.10 have in place methods for detecting and dealing with breaches of security (including loss, damage or destruction of Personal Data) including:

2.10.1 the ability to identify which individuals have worked with specific Personal Data;

2.10.2 having a proper procedure in place for investigating and remedying breaches of the data protection principles contained in the Act; and

2.10.3 notifying the Controller as soon as any such security breach occurs.

2.11 have a secure procedure for backing up and storing back-ups separately from originals;

2.12 have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print outs and redundant equipment; and

2.13 adopt such organisational, operational and technological processes and procedures as are required to comply with the requirements of ISO/IEC 27001:2013 as appropriate to the Services provided to the Controller.

_____	_____
Signature of Billy User	Signature of Billy Inc.
_____	Joshua Waldman, CEO
Typed name & Role	Typed name & Role
_____	5/1/2018
Date	Date