Data Processing Agreement
(hereunder referred to as the "**DPA**")

This DPA supplements the Harvest General Terms & Conditions (**Agreement**) between Harvest and the customer that has executed or entered in to the Agreement.

1. SCOPE

This DPA applies to the personal data processing carried out by Processor in its capacity of "processor" within the context of the performance of the Agreement and the provision of the Services.

Besides the performance of the Agreement, Processor is also controller of some data processing activities of its own, some of which being intrinsic to Processor's activities and security standards. Such data processing activities are outside the scope of this DPA.

2. DEFINITIONS

Within the context of the performance of the Agreement, and for the purposes of this DPA, the terms "Representative", "Data Subject", "Personal Data", "Processing", "Third Party", "Personal Data Breach", "Supervisory Authority" and "Data Protection Officer", shall have the meanings given to them under the Data Protection Law (as well as, in general, any other terms defined by the Data Protection Law).

3. DETAILS ON THE PROCESSING ACTIVITY

By deciding to use and by using the Services, the Controller determines the purposes and means for which personal data is processed in such a context.

The Controller is not only responsible for the Processing within the meaning of the DGPR, but also remains the main operator of the Services, the Processing that the Processor may carry out being only incidental and ancillary to the Services. The object, nature and purpose of the Processing, as well as the type of personal data processed (hereinafter the "Processed Data") and the categories of persons concerned are those defined or arising directly from the Agreement and the Services. The duration of the processing corresponds to the duration of the Agreement.

The Controller undertakes to limit as far as possible the Processing that the Processor may be required to perform in its capacity as a Processor within the framework of its Services. Unless explicitly stated otherwise, under no circumstances shall the Processed Data relate to minors and shall not include any of the sensitive data referred to in Articles 9 and 10 of the GDPR.

4. OBLIGATIONS ON ALL PARTIES

All parties shall comply with their respective obligations under the provisions of the Data Protection Law.

All parties and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

5. SPECIFIC OBLIGATIONS OF PROCESSOR

5.1 Controller's instructions

Processor shall, for the purposes of the Processing under this DPA and in respect of the provision of the Agreement, process the Processed Personal Data solely in accordance with the instructions of the Controller.

Controller hereby instructs Processor to carry out (i) any Processing necessary for the provision of the Services by Processor to Controller; and (ii) any further or ancillary Processing that Processor deems necessary to ensure provision of the Services including any support, improvement and/or development of the solutions or any other action Processor shall deem necessary at all times using appropriate technical and organizational measures. Taking into account the nature of the Services, the Agreement and the use by the Controller of the features and functionalities made available by Processor as part of the Services are the Controller's complete and final instructions to the Processor in relation to processing of personal data.

Processor, and any person acting under the authority of Processor, shall not process the Processed Personal Data except on such instructions from Controller (including with regard to transfers of Processed Personal Data outside the EU or an international organization), unless Processor is required to do so by Union or Member State law to which Processor is subject (in which case, Processor shall inform Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest).

Processor shall immediately inform Controller if, in its opinion, an instruction of Controller infringes any provision of the Data Protection Law.

5.2 Confidentiality

Processor ensures that persons authorized to Process the Processed Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.3 Security of the Processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter-alia as appropriate: (i) the pseudonymisation and encryption of the Processed Personal Data (as appropriate); (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to the Processed Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

Processor is responsible for the sufficiency of the security, privacy, and confidentiality safeguards of all personnel with respect to the Processed Personal Data and liable for any

failure by such personnel to meet the terms of this DPA. Processor takes reasonable steps to confirm that personnel are protecting the security, privacy and confidentiality of the Processed Personal Data consistent with the requirements of this DPA.

The current security measures adopted by Processor are listed in **Appendix 1**, which forms an integral part of this DPA. Controller confirms that, considering the Controller's use of Processor's Services, it deems that such measures currently meet the requirements of the GDPR and ensure the adequate protection of the rights of the data subject.

Processor shall notify Controller of any Personal Data Breach by Processor or its Sub-processors affecting the Processed Personal Data without undue delay and in any event not later than forty-eight (48) hours of becoming aware of a Personal Data Breach unless Processor is able to show that the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons. Processor shall also provide Controller with full and ongoing assistance in relation to each Party's obligations under the Data Protection Laws in accordance with any timescales reasonably required by the Controller and the Supervisory Authority concerned, when applicable.

5.4 Assignment of Sub-processors

Controller gives a general authorization to assign sub-processors.

Processor shall inform Controller if it intends or requires to engage Sub-processors (other than Existing Sub-processors, listed in **Appendix 2**, whom Processor may continue to use without the need for further approval of Controller) to help it satisfy its obligations in accordance with this DPA or the Agreement, or to delegate all or part of the Processing activities to such Sub-processors.

In such case, Processor informs Controller of its intention to engage a Sub-processor and Controller shall have the right to oppose such engagement where Controller has legitimate reason for such objection. In such case Controller shall inform Processor of any objection in writing within thirty (30) days following receipt of notice regarding the proposed change of Sub-processor. Processor shall inform Controller by notification by email to the email addresses registered for Controller's administrator in the Services. Processor ensures that the Sub-processor is committed to the same data protection obligations particularly in respect of guarantees to implement appropriate technical and organizational measures regarding the Processing activities. In any cases, Processor remains liable to Controller for the Sub-processors' acts and omissions with regard to data protection where such Sub-processors act on Processor's instructions.

5.5 Assistance for the fulfillment of Controller's obligations

5.5.1 Data subjects' rights

Data Subjects whose Personal Data are Processed have the right to request access to such Personal Data, and to request correction, erasure, blocking and/or portability of such Personal Data under conditions established by Data Protection Law. Any such requests that would be received by Processor shall be transmitted to and considered by Controller.

Taking into account the nature of the processing as described above, Processor shall assist Controller by appropriate technical and organizational measures, insofar as this is possible,

for the fulfillment of Controller's obligation to respond to requests for exercising the data subject's rights.

As part of the Services, Processor provides Controller with the ability to rectify, erase, restrict or retrieve the Processed Personal Data. Controller shall use these abilities to fulfil its obligations to respond to requests for exercising data subject's rights. In case of further assistance request from Controller, such assistance shall be invoiced by Processor to Controller as additional pay per hour work.

5.5.2 Security matters

Taking into account the nature and the information available to Processor (and remaining within its limited scope of control on the Processing), and upon specific request of Controller, Processor may assist Controller in ensuring Controller's compliance with the obligations pursuant to Articles 32 to 36 of GDPR (security obligations, obligations in case of Personal Data Breach and obligations to perform, in certain circumstances, Data Protection Impact Assessments). Such assistance is not included within the Services and shall be invoiced by the Processor to Controller as additional pay per hour work.

If the results of any possible Data Protection Impact Assessment pertaining to the processing of the Processed Personal Data and to the Services imply any substantial modification to the Services provided by Processor, Controller and Processor agree to renegotiate the terms of the Agreement accordingly (taking into account such results as well as any advice that the parties would have received from the Supervisory Authority).

5.6 Accountability and Audit

Upon Controller's request in written, Processor makes available to Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA. Where information is non-confidential or non-sensitive it will be made accessible by Controller via a straight-forward process (e.g. via the Processor's website). Where information is confidential, Processor may make it available to Controller upon request but may require Controller to first execute a non-disclosure agreement which is acceptable to Processor. Processor may in its sole discretion choose not to disclose certain high-sensitive security information. Processor may require Controller to pay a fee for information (this additional fee will be reasonable and will not be used to prevent Controller from accessing information about the security controls for the service).

If in Controller's reasonable judgment, sufficient information to confirm and demonstrate compliance with the terms of this DPA, is not provided then Controller is entitled to appoint a third-party independent auditor in the possession of the required professional qualifications and bound by a duty of confidentiality, which auditor must be reasonably acceptable to Processor, to inspect its compliance with this DPA and the Data Protection Laws required to determine the veracity and completeness of the statements submitted by Processor under this DPA.

Controller and Processor shall mutually agree upon the scope, timing, and duration of the audit. Controller shall promptly notify Processor with information regarding any non-compliance discovered during the course of an audit. Controller may not audit Processor more than once annually. Controller is responsible for all costs and fees related to such audit including, but not limited to, the professional fee of any auditor and all reasonable costs and fees for time Processor expends for any such audit, which shall be invoiced by

Processor as additional pay per hour work. All information processed or created during an Audit is Processor's confidential information. Before sharing such information with Controller, Processor may require Controller to first execute a non-disclosure agreement which is acceptable to Processor.

If a Supervisory Authority requires an audit of the Services in order to ascertain or monitor Controller's compliance with Data Protection Laws, Processor will cooperate with such audit. Likewise, Controller shall be responsible for the costs of such an audit.

5.7 End of the provision of Services relating to processing

Processor deletes or returns (in accordance with the terms and conditions set forth in the main Agreement), all the Processed Personal Data to Controller after the end of the provision of Services relating to processing or in case of Termination of the DPA, and deletes existing copies unless Union or Member State law applicable to Processor requires storage of the Processed Personal Data. Processor shall not thereafter Process such Personal Data.

6. DURATION

This DPA shall commence on the Effective Date and shall remain in force thereafter for as long as the Agreement remains in full force and effect or unless terminated by either Party in accordance with Section 7 herein.

7. TERMINATION

This DPA terminates in any cases when the Agreement terminates.

Notwithstanding anything else contained herein, the following will be considered as causes of early termination of this DPA, which will give the parties the right, at their election and in addition to whatsoever other remedies which they may have in law, to terminate this DPA with immediate effect by way of written notification to the other parties:

- Failure to fulfil any of the obligations set out in this DPA, such a failure not having been remedied within thirty (30) days of written notification to the party in breach specifying the failure to comply and seeking fulfilment thereof; or

- The extinction of the legal personality of any of the parties, suspension of payments, judicial commencement of insolvency proceedings or declaration of bankruptcy or any other situation of insolvency.

8. DISCLOSURES

Processor will not disclose Personal Data Processed pursuant to the Agreement and this

DPA to any third party, or category of third party without Controller's consent, unless Union or Member State law applicable to Processor requires otherwise.

9. RESERVATION OF RIGHTS

Controller hereby confirms warrants and agrees that it does not and will not assert or claim any interest or rights in any way under Data Protection Laws or otherwise in respect of any Processing of Personal Data under any other part(s) of the Services or of the Services than the Processed Personal Data, and Processor reserves its rights in respect of same.

10. MISCELLANEOUS

Unless specifically amended in this DPA, the Agreement remains in full force. If there is any conflict or inconsistency between the provisions of the Present DPA and any of the provisions of the Agreement, the provisions of this DPA shall prevail.

The purpose of this DPA is to secure an adequate level of protection for the Data Subjects' Personal Data. It is the intention of the Parties that this DPA shall be interpreted in the light of Data Protection Laws.

11. GOVERNING LAW

This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Laws.

12. NOTICES

Any notice or other communication under this DPA shall be in writing and shall only be considered valid if sent first by e-mail and then by registered mail to the relevant e-mail and address given above.

APPENDIX 1:
HARVEST TECHNOLOGY PTY LTD's Technical and Organizational Measures to Secure Data

Measure	Description
Measures of pseudonymisation and encryption of personal data	**Data Encryption** Entire database is encrypted. Additionally, passwords are stored in the database as hashed representations, and the password itself is not recoverable or stored. All other information is stored as raw text.
Measures for ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services	**Security Program** Harvest will maintain a security management program that includes but is not limited to: (a) executive review, support and accountability for all security related policies and practices; (b) a written information security policy and framework; (c) periodic risk assessments systems processing personal data; (d) prompt review of security incidents affecting the security of Harvest systems processing customer personal data; (e) a formal controls framework based on formal audit standards of ISO9001; (f) processes to identify and evaluate security risks, develop mitigation plans, which will be captured in the Harvest Operations Risk Matrix; and (g) a comprehensive security testing methodology that consists of diverse and independent approaches. Harvest will periodically review, test and, where applicable, update such security management program. **Security Incident Notification** Harvest will notify affected parties of security incidents in accordance with Data Processing Addendum. **Employee Screening, Training, Access & Controls** Harvest will maintain policies and practices that include the following controls and safeguards applied to Harvest employees who have access to customer personal data and/or provide support and services to the customer: (a) pre-hire background checks in accordance with applicable Laws and generally accepted industry standards; (b) periodic security awareness training; (c) a disciplinary policy and process to be used when Harvest employees breach Harvest's security policies; (d) access to Harvest IT systems only from approved Harvest-managed devices or approved and registered personal devices with appropriate technical security controls (including two-factor authentication);and

	(e) access and disclosure of information must be controlled and will only be given to employees in order to perform their duties ('need to know') or through legislation.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	**Resilience Program** During the Subscription Term, Harvest's Disaster Recovery Plan and Harvest's Backup Standard will address at least the following topics: (a) the availability of human resources with appropriate skill sets; (b) the availability of all IT infrastructure, telecommunications capabilities and any other technology used or relied upon by Harvest in the provision of the Products; (c) Harvest's plans for storage and continuity of use of data and software; (d) clear recovery time objectives (RTOs) and recovery point objectives (RPOs); (e) mechanisms for the geographic diversity or back-up of business operations; (f) the potential impact of cyber events and Harvest's ability to maintain business continuity in light of such events, as well as a framework and procedure to respond to and remediate such events; and (g) the management of data corruption incidents. Harvest will periodically (and, in any event, no less frequently than annually) review, test and, where applicable, update the Disaster Recovery Plan and Backup Standard.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	**Compliance Program** Harvest will maintain a compliance program that includes independent third-party audits and certifications. **Vulnerability Management** Harvest will maintain the following vulnerability management processes: *Vulnerability Scanning and Remediation*. Harvest conducts frequent vulnerability scanning to test its network and infrastructure and application vulnerability testing to test its applications and services in accordance with its Network Security & Management Standard. Harvest applies security patches to software components in production and development environments as soon as commercially practicable. *Identifying Malicious Threats*. Harvest employs processes and tools in line with industry standards to identify malicious actors and prevent them from accessing customer personal or Harvest systems that process customer personal data. These include, but are not limited to, maintaining software that attempts to identify and detect attempted intrusions, behaviours consistent with internet-based attacks, and

	indicators of potential compromise. Harvest has a security incident processes to notify appropriate personnel in response to threats. *Vulnerability Testing.* (a) Harvest conducts internal vulnerability testing, as described here. This includes identifying and fixing bugs according to risk and priority. (b) Harvest will use commercially reasonable efforts to address identified security vulnerabilities in our products.

APPENDIX 2:
List of HARVEST TECHNOLOGY PTY LTD's current sub-processors

Sub-processor	**Purpose**	**Entity Country**	**Website**
Amazon Web Services, Inc	Data hosting	Australia, Ireland, USA	https://aws.amazon.com
Digital Ocean	Data hosting	USA	Htts://www.digitalocean.com
Dropbox International Unlimited Company	File hosting services	Ireland, USA	https://dropbox.com
Freshworks / Freshdesk	Customer service and support	Australia, Germany, India, UK, USA	https://www.freshworks.com/freshdesk/
Hotjar Ltd	Web analytics	Malta	https://www.hotjar.com
Google Ireland Limited	Web analytics	Ireland	https://analytics.google.com
Microsoft Corporation	Email service provider and file hosting services	Ireland, USA	https://microsoft.com
OVH Australia Pty Ltd	Data hosting	Australia	https://www.ovhcloud.com/en-au/

Rocketgenius, Inc. dba Gravity Forms	Customer service	USA	https://gravityforms.com
SFDC Australia Pty Ltd (Salesforce)	Account management CRM	Australia	https://www.salesforce.com
SAP Australia Pty Ltd	Account management CRM	Australia	https://www.sap.com/australia/index.html
Stripe Payments Australia Pty Ltd	Payment Gateway	Australia	https://stripe.com/au/
The Rocket Science Group LLC d/b/a Mailchimp	Marketing email service provider	USA	https://mailchimp.com