Harvest Data Processing Agreement

Last updated: 17 April 2025

This Data Processing Agreement forms part of, and is subject to, the Agreement between the Customer and Harvest and reflects the parties' agreement with respect to the Processing of Customer Personal Data.

1. Definitions and Interpretation

1.1 Defined terms have the meaning given to them throughout this Data Processing Agreement, in the Agreement, and as follows.

Agreement means the agreement formed between Harvest and the Customer under the Harvest General Terms and Conditions.

Contracted Processor means the Data Processor or a Subprocessor.

Customer means the customer of Harvest's Services as referred to in the Harvest General Terms and Conditions.

Customer Personal Data means any Personal Data Processed by a Contracted Processor on behalf of the Customer pursuant to or in connection with the Agreement.

Data Processor means Harvest.

Data Protection Laws means:

(a) the DPA;

(b) the EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR; and

(c) to the extent applicable, the data protection or privacy laws of any other country.

DPA means the Data Protection Act 2018 (UK) as amended, updated, or replaced from time to time, and includes the UK GDPR as defined in section 3 of the Data Protection Act 2018 (UK).

EEA means the European Economic Area.

EU means the European Union.

EU C-to-P SCCs means the EU approved Controller to Processor standard contractual clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021, available at: https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en, as amended, updated, or replaced from time to time.

GDPR means Regulation 2016/679 (the General Data Protection Regulation), as amended, updated, or replaced from time to time.

Harvest refers to the Harvest entity the Customer purchases the Services from, being one of the following:

(a) Harvest Technology Pty Ltd (ABN 52 601 194 138) of 7 Turner Avenue, Technology Park, Bentley, Western Australia, Australia;

(b) Harvest Technology (UK) Ltd (Company Number 14032351) of 71-75 Shelton Street, Covent Garden, London WC2H 9JQ, United Kingdom; or

(c) Harvest Infinity Pty Ltd (ABN 57 620 773 060) of 7 Turner Avenue, Technology Park, Bentley Western Australia.

Harvest General Terms and Conditions means the then-current version of the terms and conditions located at https://harvest.technology/terms-and-conditions.

Data Transfer means:

(d) a transfer of Customer Personal Data from the Customer to a Contracted Processor; or

(e) an onward transfer of Customer Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws).

ICO means the UK Information Commissioner.

Services means means Harvest's provision of goods and services to Customer in accordance with the terms of the Agreement.

Standard Contractual Clauses means, as applicable the EU C-to-P SCCs and/or the UK SCCs.

Subprocessor means any person appointed by or on behalf of the Data Processor to Process Personal Data on behalf of the Customer in connection with the Agreement or the Data Processing Agreement in accordance with clause 6, including those Subprocessors set out at Appendix C to this Data Processing Agreement.

UK means the The United Kingdom of Great Britain and Northern Ireland.

UK SCCs the UK standard data protection clauses as issued by the ICO under s119(A)(1) of the DPA, as amended, updated, or replaced from time to time.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" have the same meaning as in the relevant Data Protection Laws.

2. Application

2.1 The parties agree that in the event of inconsistency, the terms of this Data Processing Agreement override the terms of the Agreement.

2.2 Nothing in this Data Processing Agreement reduces the either party's obligations under the Agreement or permits the Data Processor to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by any applicable law.

2.3 For the purposes of this Data Processing Agreement, Harvest is a Data Processor and Customer is the Controller.

3. Processing of Customer Personal Data

3.1 Data Processor will:

(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 documented instructions of Customer, which for the purpose of this Data Process Agreement include the Customer's instructions to Process Customer Personal Data to provide the Services.

4. Duration

This Data Processing Agreement, and the Data Processor's Processing of Customer Personal Data, will continue unless or until the Agreement expires or is terminated.

5. Data Processor Personnel

Data Processor will take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Customer Personal Data, ensuring in each case that 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 Agreement and the Services, and to comply with all applicable laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. Security

6.1 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, Data Processor must, in relation to Customer Personal Data, implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

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

6.3 The current security measures adopted by the Data Processor are listed in Appendix B. Controller agrees that such measures meet the requirements of Article 32(1) of the GDPR and ensure the adequate protection of the rights of the data subject.

7. Subprocessing

7.1 The Data Controller grants the Data Processor a general authorisation to appoint, use, and disclose Customer Personal Data to, any Subprocessor set out in Appendix B to this Data Processing Agreement and/or any other Subprocessor added to Appendix B from time to time in accordance with clause 7.2.

7.2 The Data Processer may appoint a new subprocessor by providing the Customer with 30 days notice (**Change Notice Period**) and, such new subprocessor will be deemed a Subprocessor and added to the list set out at Appendix B, unless the Customer objects to the appointment on reasonable grounds and in accordance with the following process.

(a) If the Customer objects to the appointment of the new Subprocessor, the Customer must do so in writing to the Data Processor before the expiry of the Change Notice Period and the parties will discuss those objections in good faith.

(b) If it can be reasonably demonstrated by the Customer that the new Subprocessor is unable to Process Personal Information in compliance with the terms of this Data Processing Agreement, and the Data Processor cannot provide an alternative subprocessor, or the parties are not otherwise able to achieve a resolution, then:

(i) the Data Processor will cease to provide, or Customer may agree not to use (temporarily or permanently), the aspect of the Services that would involve the Subprocessor Processing Customer Personal Data; or

(ii) if the Customer is no longer able to use the Services without the appointment of the new subprocessor, the Customer may terminate the Agreement and this Data Processing Agreement, subject to any effect of termination provisions in the Agreement.

(c) Where the Customer fails to object within the Change Notice Period, the Customer will be deemed to have consented to the appointment of the relevant Subprocessor.

7.3 The Data Processor must ensure that it has a written agreement in place with each Subprocessor that imposes similar standards and obligations on the Subprocessor as those set out in this Data Processing Agreement in respect of the Processing of Customer Personal Data carried out by that Subprocessor.

8. Data Subject Rights

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

8.2 Data Processor must:

(a) promptly notify the Customer if it receives a request from a Data Subject under any 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 Customer or as required by applicable laws to which the Data Processor is subject, in which case Data Processor will, to the extent permitted by applicable laws, inform the Customer of that legal requirement before the Contracted Processor responds to the request.

9. Personal Data Breach

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

9.2 Data Processor will co-operate with the Customer and take reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

10. Data Protection Impact Assessment and Prior Consultation

10.1 Data Processor will provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which the Customer reasonably considers to be required by Articles 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10.2 Such reasonable assistance is not included within the Services and the Data Processor may invoice the Controller for providing such assistance, at the Data Processor's then-current time and materials hour rates.

11. Deletion or return of Customer Personal Data

11.1 Except to the extent that the Data Processor is required to retain any Customer Personal Data under any applicable Data Protection Laws and/or other laws, codes or regulations, the Data Processor must promptly, and in any event within 30 business days of the date of cessation of any Services involving the Processing of Customer Personal Data (the **Cessation Date**), delete and procure the deletion of all copies of such Customer Personal Data, which the Customer acknowledges may include cryptographically deleting data so as to render it unreadable.

11.2 Data Processor will provide written certification to the Customer that it has fully complied with this clause within 10 business days of the Cessation Date.

12. Audit rights

12.1 On request, the Data Processor will make available to the Customer all information necessary to demonstrate compliance with this Data Processing Agreement, and will allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the

Customer in relation to the Processing of Customer Personal Data by the Contracted Processors.

12.2 Information and audit rights of the Customer only arise under clause 12.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

13. Data Transfer

General

13.1 Data Processor may not transfer or authorize the transfer of Customer Personal Data to countries outside the UK, the EU and/or the EEA without the prior written consent of the Customer, and subject to the relevant provisions of this clause 13.

13.2 For the purposes of the agreement and this Data Processing Agreement, the Customer explicitly consents to the transfer of Customer Personal Data to Australia, Singapore, the UK (for EU Personal Data), and the United States of America.

13.3 The parties agree that formation of the Agreement to which this Data Processing Agreement relates will be considered as signature to the applicable Standard Contractual Clauses.

13.4 If Personal Data Processed under this Data Processing Agreement is transferred from a country within the:

(a) UK; or

(b) EEA

to (respectively) a country outside the:

(c) UK; and/or

(d) EEA,

the parties will ensure that the Personal Data is adequately protected. To achieve this, the parties will, unless agreed otherwise, rely on the then current, applicable and approved Standard Contractual Clauses and the relevant Standard Contractual Clauses are deemed to be incorporated into, and form part of, this Data Processing Agreement, subject to the applicable adapations set out below.

All Standard Contractual Clauses.

13.5 If so required by the laws or regulatory procedures of any jurisdiction, the parties will execute or re-execute the relevant Standard Contractual Clauses as separate documents setting out the proposed transfers of Personal Data in such manner as may be required.

13.6 In the event of inconsistencies between the provisions of the relevant Standard Contractual Clauses and this Data Processing Agreement or other agreements between the parties in relation to the Services, the the relevant Standard Contractual Clauses will take precedence.

The terms of this Data Processing Agreement will not vary the the relevant Standard Contractual Clauses in any way.

UK SCCs

13.7 References to the GDPR are to be understood as references to the either the GDPR or the DPA as the context requires and as applicable insofar as data transfers are subject to these laws.

13.8 For the purposes of Table 2 of the UK SCCs ("Selected SCCs, Modules and Selected Clauses"), the EU C-to-P SCCs, as read together with the UK SCCs, will apply.

13.9 For the purpose of Table 3 of the UK SCCs ("Appendix Information") Appendixes A, B and C to this Data Processing Agreement also apply.

13.10 The UK SCCs will be governed by the laws of Great Britain. Any dispute arising from the UK SCCs in relation to all data transfers will be resolved by the courts of Great Britain.

EU C-to-P SCCs

13.11 The docking clause 7 of the EU C-to-P SCCs will be included.

13.12 The option in clause 11 EU C-to-P SCCs will be waived.

13.13 For clauses 17 and 18 of the EU C-to-P SCCs, the EU C-to-P SCCs will be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they will be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this will be the law of Ireland (specify Member State). Any dispute arising from the EU C-to-P SCCs will be resolved by the courts of an EU Member State. The parties agree that those will be the courts of EU Member State in which the data exporter is established. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence. The parties agree to submit themselves to the jurisdiction of such courts.

13.14 For the purposes of Annex I of the Appendix to the EU C-to-P SCCs, the parties and processing details set out in Appendix A to this Data Processing Agreement will apply.

13.15 For the purposes of Annex II of the of the Appendix to the EU C-to-P SCCs, the technical security measures set out in Appendix B to this Data Processing Agreement will apply.

13.16 For the purposes of Annex III of the of the Appendix to the EU C-to-P SCCs, the list of subprocessors set out in Appendix C to this Data Processing Agreement, and clause 7, will apply.

14. Variations

14.1 Where a variation does not result in the protection of Customer Personal Data being as, or more, rigorous than what is set out in this Data Processing Agreement (as updated or amended in accordance with this clause 14), Harvest may, from time to time, vary this Data Processing Agreement by notice via email to the relevant contact person set out in the Agreement. The

Customer's continued use of Harvest's Services will be deemed as acceptance of such variation.

14.2 In all other circumstances, this Data Processing Agreement can only be varied by written agreement by the parties. The date set out at the start of this Data Protection Agreement will indicate the date it was last updated.

15. General Terms

This Data Processing Agreement is governed by the laws that govern the Agreement. Any dispute arising in connection with this Data Processing Agreement will be submitted to the non-exclusive jurisdiction of the courts that have jurisdiction in the Agreement.

Appendix A to Data Processing Agreement – Parties and Processing Details

1 Description of parties

1.1 Data exporter(s): Data exporter is the Customer.

1.2 Data importer(s): Data importer Harvest.

2 Description of transfer

2.1 Categories of data subjects whose personal data is transferred:

Customers, employees who fulfil an operational function in relation to the Services, resellers, customer's employees, contractors and clients, and the employees and contractors of Customer's clients.

2.2 Categories of personal data transferred:

The personal data transferred concern the following categories of data:

- General personal data categories, such as name, date of birth, company and job title/role, and your contact information including phone number and email address

2.3 The personal data transferred concern the following special categories of data:

NIL

2.4 The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous basis for the duration of this Data Processing Agreement.

2.5 Nature of the processing:

The personal data transferred will be subject to the following basic processing activities:

- Collection by the Customer from data subjects; disclosure to Harvest; hosting and storage by Harvest in Subprocessor servers; processing for the purposes set out below; retention in accordance with this Data Processing Agreement.

2.6 Purpose(s) of the data transfer and further processing:

The purposes of Harvest providing the Services and on the documented instructions of Customer.

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

In accordance with clause 11 of this Data Processing Agreement.

2.8 For transfers to subprocessors, also specify subject matter, nature and duration of the processing.

As above.

3 Description of competent supervisory authority

3.1 Identify the competent supervisory authority/ies.

The supervisory authority of the EU Member State where the data exporter is established, or where the data exporter is established in the UK, then the ICO.

Appendix B to Data Processing Agreement – Technical Security Measures

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 C to Data Processing Agreement – Subprocessors

The controller has authorised the use of the following subprocessors.

List of Subprocessors

Sub-processor	Purpose	Entity Country	Website
Amazon Web Services, Inc	Infrastructure hosting, SES email delivery, cloud storage, and processing	Australia, Ireland, USA	https://aws.amazon.com
Digital Ocean	Infrastructure hosting, 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 Limited	Website SEO/Ads/Analytics/reCAPTCHA	Ireland USA	https://www.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	Marketing email service provider	USA	https://mailchimp.com

Group LLC d/b/a Mailchimp			
Keptago Ltd	Address autocomplete	Cyprus	https://www.geoapify.com