dovetail

Data Processing Agreement (DPA)

This DPA is entered into between us and the Customer and is incorporated into and governed by the terms of our Customer Terms of Service at https://dovetailapp.com/legal/customer-terms.

1. Definitions

Any capitalised term not defined in this DPA shall have the meaning given to it in the Customer Terms of Service.

"Customer Terms"	means the agreement between us and the Customer for the provision of the Services;
"Controller"	means you, the Customer;
"Data Subject"	shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (as amended from time to time, or replaced by subsequent legislation);
"DPA"	means this Data Processing Agreement together with its Appendix 1 and the Security Documentation, linked below;
"Personal Data"	shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (as amended from time to time, or replaced by subsequent legislation);
"Processor"	means us, Dovetail;
"Security Documentation"	means the security documents located at https://dovetailapp.com/product/security as amended from time to time, or as otherwise made available by the Processor to the Controller;

“Standard Contractual Clauses”	means the EU model clauses for Personal Data transfer from controllers to processors c2010-593 - Decision 2010/87EU;
“Subsidiary”	means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party;
“Sub-Processor”	means any person or entity engaged by us (including a Subsidiary) to process Personal Data in the provision of the Services to the Customer.

2. Purpose

The Processor has agreed to provide the Services to the Controller in accordance with the terms of the Customer Terms.

In providing the Services, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

3. Scope

In providing the Services to the Controller pursuant to the terms of the Customer Terms, the Processor shall process Personal Data only to the extent necessary to provide the Services in accordance with both the terms of the Customer Terms and the Controller’s instructions documented in the Customer Terms and this DPA.

4. Processor Obligations

The Processor may collect, process or use Personal Data only within the scope of this DPA.

The Processor confirms that it shall process Personal Data on behalf of the Controller and shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process the Personal Data except on instructions from the Controller.

The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breach any applicable data protection laws.

The Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data:

a. are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential;
b. have received appropriate training on their responsibilities as a data processor; and
c. are bound by the terms of this DPA.

The Processor shall implement appropriate technical and organisational procedures to protect Personal Data, 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 shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

a. the pseudonymisation and encryption of Personal Data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

The technical and organisational measures detailed in the Security Documentation shall be at all times adhered to as a minimum security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA provided that such updates and modifications do not result in the degradation of the overall security of the Services.

Where Personal Data relating to an EU Data Subject is transferred outside of the EEA it shall be processed only by entities which:

a. are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or
b. have entered into Standard Contractual Clauses with the Processor; or
c. have other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data.

5. Controller Obligations

The Controller represents and warrants that it shall comply with the terms of the Customer Terms, this DPA and all applicable data protection laws.

The Controller represents and warrants that it has obtained any and all necessary permissions and authorisations necessary to permit the Processor, its Subsidiaries and Sub-Processors, to execute their rights or perform their obligations under this DPA.

The Controller is responsible for compliance with all applicable data protection legislation, including requirements with regards to the transfer of Personal Data under this DPA and the Customer Terms.

All Subsidiaries of the Controller who use the Services shall comply with the obligations of the Controller set out in this DPA.

The Controller has their own obligations to implement their own appropriate technical and organisational procedures to protect Personal Data, 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 Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

a. the pseudonymisation and encryption of Personal Data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In accessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

The Controller shall take steps to ensure that any natural person acting under the authority of the Controller who has access to Personal Data does not process the Personal Data except on instructions from the Controller.

The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Customer Terms. The Processor will process the request to the extent it is lawful, and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.

The Controller acknowledges and agrees that some instructions from the Controller, including destruction or return of data from the Processor, may result in additional fees. In such case, the Processor will notify the Controller of such fees in advance unless otherwise agreed.

6. Sub-Processors

The Controller acknowledges and agrees that:

a. Subsidiaries of the Processor may be used as Sub-Processors; and
b. the Processor and its Subsidiaries respectively may engage Sub-Processors in connection with the provision of the Services.

All Sub-Processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor similar to those set out in this Data Processing Agreement.

Where Sub-Processors are located outside of the EEA, the Processor confirms that such Sub-Processors:

a. are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or
b. have entered into Standard Contractual Clauses with the Processor; or
c. have other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

The Processor shall make available to the Controller the current list of Sub-Processors (at https://dovetailapp.com/legal/data-subprocessors) which shall include the identities of Sub-Processors, what they're used for, and their location.

During the term of this DPA, the Processor shall provide the Controller with at least 14 days prior notification, via email (or in-application notice), of any changes to the list of Sub-Processor(s) who may process Personal Data before authorising any new or replacement Sub-Processor(s) to process Personal Data in connection with the provision of the Services.

If the Controller objects to a new or replacement Sub-Processor the Controller may terminate the Customer Terms with respect to those Services which cannot be provided by the Processor without the use of the new or replacement Sub-Processor. The Processor will refund the Controller any prepaid fees covering the remainder of the Term of the

Customer Terms following the effective date of termination with respect to such terminated Services.

7. Liability

The limitations on liability set out in the Customer Terms apply to all claims made pursuant to any breach of the terms of this DPA.

The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-Processors to the same extent the Processor would be liable if performing the services of each Sub-Processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Customer Terms.

The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Subsidiaries as if such acts, omissions or negligence had been committed by the Controller itself.

8. Audit

The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Customer Terms. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may at its own expense conduct a more extensive audit which will be:

a. limited in scope to matters specific to the Controller and agreed in advance with the Processor;
b. carried out during Australian business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and
c. conducted in a way which does not interfere with the Processor's day-to-day business.

The Processor may charge a fee (based on its reasonable time and costs) for assisting with any audit. The Processor will provide the Controller with further details of any applicable fee, and the basis of its calculation, in advance of any such audit.

This clause shall not modify or limit the rights of audit of the Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

9. Data Deletion

The Controller will enable the Processor to delete Personal Data using the functionality provided by the Service. For certain deletions, a recovery feature is offered by the Processor to enable recovery from accidental deletions for up to 14 days. This may be overridden by the Processor. After any recovery period, the Processor will permanently delete the Personal Data from the live systems.

On termination, the Controller has the option to request the return or deletion of Personal Data. This request must be made within 14 days of termination. The Processor will make the data available for download by the Controller in a machine readable format. Thereafter the Processor will permanently delete the Personal Data from the live systems in any event.

Following permanent deletion from the live systems, partial data resides on the Processor's archival systems for a period of up to 14 days. If requested by the Controller, the Processor may be able to assist with recovery of partial data from these archives during this period. A fee will be charged for this service.

10. Notification of Data Breach

The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data (**"Data Breach"**).

The Processor will take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Data Breach and to assist the Controller in meeting the Controller's obligations under applicable law.

The Processor's notification of, or response to, a Data Breach under this Section 10 will not be construed as an acknowledgement by the Processor of any fault or liability with respect to the Data Breach.

The Processor will not assess the content of the Controller's data in order to identify information subject to any specific Controller data breach. Controller is solely responsible for complying with data breach notification laws applicable to the Controller and fulfilling any third party notification obligations related to any Data Breach(es).

11. Compliance, Cooperation and Response

In the event that the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law. The Controller shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request or assisting the Controller in complying with its duties. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable.

The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller, unless such notification is not permitted under applicable law or a relevant court order.

The Processor may make copies of and/or retain Personal Data in order to comply with its legal or regulatory requirement including, but not limited to, retention requirements.

The parties acknowledge that it is the duty of the Controller to notify the Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the parties agree that amendments are required, but the Processor is unable to accommodate the necessary changes, the Controller may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.

The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a supervisory data protection authority in the performance of their respective obligations under this DPA.

The parties agree that the Processor will be entitled to charge the Controller additional fees to reimburse the Processor for its staff time, costs and expenses in assisting the Controller, when the Controller requests the Processor to provide assistance pursuant to this DPA. In such cases, the Processor will notify the Controller of its fees for providing assistance, in advance.

12. Term and Termination

The term of this DPA shall coincide upon receipt of the validly completed DPA. This DPA shall terminate automatically together with termination or expiry of the Customer Terms.

13. General

This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

This DPA shall be governed by the law of Australia. The courts of Australia shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

The parties' authorized signatories have duly executed this DPA:

On behalf of Controller:

Name (written out in full):	
Position:	
Company:	
Address:	
Date:	
Signature:	

On behalf of Processor:

Name (written out in full):	Benjamin Humphrey
Position:	Chief Executive Officer
Company:	Dovetail Research Pty Ltd
Address:	8/6 Holbrook Avenue, Kirribilli, 2061, NSW, Australia
Signature:	

Appendix 1

Overview of data processing activities to be performed by the Processor.

1. Controller

The Controller transfers Personal Data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below. The Controller is the Customer.

2. Processor

The Processor received data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below. The Processor is:

Dovetail Research Pty Ltd, a private limited company registered in Australia with Australian Business Number (ABN) 84 615 270 025, with its registered office at 8/6 Holbrook Avenue, Kirribilli, 2061, NSW, Australia.

3. Data Subjects

The Personal Data transferred includes but is not limited to the following categories of Data Subjects:

Individuals about whom data is uploaded to the Service by (or at the direction of) the Controller or by Users, Subsidiaries and other participants whom the Controller has granted the right to access the Service in accordance with the provisions of the Customer Terms.

4. Categories of Data

The Personal Data transferred includes but is not limited to the following categories of data:

Data relating to individuals uploaded to the Service by (or at the direction of) the Controller or by Users, Subsidiaries and other participants whom the Controller has granted the right to access the Service in accordance with the provisions of the Customer Terms.

5. Special Categories of Data

Personal Data transferred includes but is not limited to the following special categories of data:

No sensitive or special categories of data are permitted to be transferred and shall not be contained in the content of attachments to emails.

6. Processing Operations

The Personal Data transferred will be subject to the following basic processing activities:

a. Personal Data will be processed to the extent necessary to provide the Service in accordance with both the Customer Terms and the Controller's instructions. The Processor processes Personal Data only on behalf of the Controller. Processing operations include, but are not limited to the provision of the Service – this operation relates to all aspects of Personal Data processed.
b. Technical support, issue diagnosis and error correction to ensure the efficient and proper running of the systems and to identify, analyse and resolve technical issues both generally in the provision of the Service and specifically in answer to a Controller query. This operation may relate to all aspects of Personal Data processed but will be limited to metadata where possible.
c. URL scanning for the purposes of the provision of targeted threat protection and similar service which may be provided under the Customer Terms. This operation relates to attachments and links in emails and will relate to any Personal Data within those attachments or links which could include all categories of Personal Data.