This DPA is entered into between the Company and the Customer and is incorporated into and governed by the Terms of the Agreement.

1. Definitions

Any capitalized term not defined in this DPA shall have the meaning given to it in the Agreement.

Term	Definition
“Affiliates”	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;
“Agreement”	means the agreement between the Company and the Customer for the provision of the Services;
“Controller”	means 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 Exhibits A and B;
“Notifiable Personal Data Breach”	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which is likely to result in a risk to the rights and freedoms of natural persons;
“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 the Company;
“Security Policy”	means the Company’s security document as updated from time to time and is available on request.
“Standard Contractual	means the EU model clauses for personal data transfer from controllers to processors c2010-593 - Decision 2010/87 EU;

Clauses”	
“Sub-Processor”	means any person or entity engaged by the Company or an Affiliate to process Personal Data in the provision of the Services to the Customer.

2. Purpose

2.1 The Processor has agreed to provide the Services to the Controller in accordance with the terms of the Agreement. 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

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

4. Processor Obligations

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

4.2 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 shall only process the Personal Data on the documented instructions of the Controller.

4.3 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.

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

(i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential;

(ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.

4.5 The Processor shall implement appropriate technical and organizational 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.

4.6 The 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 encryption of Personal Data;

(ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;

(iii) the ability to restore the availability and access to 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.

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, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

4.7 The technical and organizational measures detailed in Exhibit B shall be at all times adhered to as a minimum-security standard. The Controller accepts and agrees that the technical and organizational 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.

4.8 The Controller acknowledges and agrees that, in the course of providing the Services to the Controller, it may be necessary for the Processor to access the Personal Data to respond to any technical problems or Controller queries and to ensure the proper working of the Services. All such access by the Processor will be limited to those purposes.

4.9 Where Personal Data relating to an EU Data Subject is transferred outside of the EEA it shall be processed in accordance with the provisions of the Standard Contractual Clauses, unless the processing takes place: (i) in a third country or territory recognized by the EU Commission to have an adequate level of protection; or (ii) by an organization located in a country which has other legally recognized appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

4.10 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 organizational 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

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

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

5.3 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 Agreement.

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

5.5 The Controller shall implement appropriate technical and organizational 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 organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(i) the encryption of Personal Data;

(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 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.

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, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

5.6 The Controller shall take steps to ensure that any natural person acting under the authority of the Controller who has access to Personal Data only processes the Personal Data on the documented instructions of the Controller.

5.7 The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. 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.
5.8 The Controller acknowledges and agrees that some instructions from the Controller, including destruction or return of data, assisting with audits, inspections or DPIAs by the Processor, may result in additional fees. In such case, the Processor will notify the Controller of its fees for providing such assistance in advance, unless otherwise agreed.

6. Sub-Processors

6.1 The Controller acknowledges and agrees that:

(i) Affiliates of the Processor may be used as Sub-processors; and

(ii) the Processor and its Affiliates respectively may engage Sub-processors in connection with the provision of the Services.

6.2 All Sub-processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor set out in this DPA.
6.3 Where Sub-processors are located outside of the EEA, the Processor confirms that such Sub-processors:

(i) are located in a third country or territory recognized by the EU Commission to have an adequate level of protection; or

(ii) have entered into Standard Contractual Clauses with the Processor; or (iii) have other legally recognized appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

6.4 The Processor shall make available to you the current list of Sub-processors at http://bigmind.zoolz.com/dpa-subprocessors which shall include the identities of Sub-processors and their country of location. During the term of this DPA, the Processor shall provide the Controller with prior notification, via email, of any changes to the list of Sub-processors(s) who may process Personal Data before authorizing any new or replacement Sub-processor(s) to process Personal Data in connection with the provision of the Services.
6.5 The Controller may object to the use of a new or replacement Sub-processor by notifying the Processor promptly in writing within ten (10) Business Days after receipt of the Processor's notice. If the Controller objects to a new or replacement Sub-processor, and that objection is not unreasonable, the Controller may terminate the Agreement 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 Agreement following the effective date of termination with respect to such terminated Services.

7. Liability

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

7.2 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 Agreement.

7.3 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 Affiliates as if such acts, omissions or negligence had been committed by the Controller itself.

7.4 The Controller shall not be entitled to recover more than once in respect of the same claim.

8. Audit

8.1 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. Further information about the audit process is available on request.

8.2 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 Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may conduct a more extensive audit which will be:

(i) at the Controller's expense;

(ii) limited in scope to matters specific to the Controller and agreed in advance;

(iii) carried out during UK business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and

(iv) conducted in a way which does not interfere with the Processor's day-to-day business. The Controller shall provide the Processor with a copy of the audit report within 14 days of the audit being completed.

8.3 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. Notification of Notifiable Personal Data Breach

9.1 The Processor shall notify the Controller without undue delay after becoming aware of any Notifiable Personal Data Breach.

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

10. Compliance, Cooperation and Response

10.1 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. 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.

10.2 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.

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

10.4 The Processor shall reasonably assist the Controller in meeting its obligation to carry out data protection impact assessments (DPIAs), taking into account the nature of processing and the information available to the Processor.

10.5 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 organizational 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.

10.6 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.

11. Term and Termination

11.1 The Processor will only process Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

11.2 The Processor shall at the choice of the Controller, delete or return Personal Data to the Controller. If the Controller wishes to have Personal Data returned, they must themselves export the Personal Data from within the App prior to cancelling their subscription. 30 days after the termination of the subscription all Personal Data within the App will be automatically and permanently deleted by the Company unless applicable law or regulations require storage of the Personal Data.

12. General

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

12.2 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.

12.3 This DPA shall be governed by the laws of England and Wales. The courts of England shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

12.4 This DPA is incorporated into and governed by the terms of the Agreement.

Exhibit A

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 named in the Sign-Up Form and is referred to as the Account Owner.

2. Processor

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

3. Data Subjects

The Personal Data transferred concern the following categories of Data Subjects:

- Employees, freelancers and contractors of the Controller.
- Authorized Users, Affiliates and other participants from time to time to whom the Controller has granted the right to access the Services in accordance with the terms of the Agreement.
- Clients of the Controller and individuals with whom those end users communicate with by email and/or instant messaging.
- Service providers of the Controller.
- Children who are at least 16 years old
- Other individuals to the extent identifiable in the content of emails or their attachments or in archiving content.

4. Categories of Data

The Personal Data transferred concern the following categories of data:

- Personal details, names, usernames, passwords, email addresses
- Personal Data derived from Authorized Users use of the Services such as records and business intelligence information
- Personal Data within email and messaging content which identifies or may reasonably be used to identify, data subjects
- Metadata including sent, to, from, date, time, subject, which may include Personal Data
- Financial data

- Data concerning profession and employment data.

5. Special categories of Data

Personal Data transferred concern the following special categories of data:

- No sensitive data or special categories of data are intended to be transferred but may be contained in the content of or attachments to emails.
- The Services do not require the acquisition, storage and processing of sensitive data for the purpose of report production. Therefore, if this data is entered, then it would be deemed a breach of these terms and the Data Controller would not accept any resultant liability.

6. Processing operations

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

- Personal Data will be processed to the extent necessary to provide the Services in accordance with both the Agreement and the Controller's instructions. The Processor processes Personal Data only on behalf of the Controller. Processing operations include, but are not limited to:
- Acquisition and storage of Customer credential data so that the Customer can use the Services.
- Acquisition and storage of Client data so the Customer can write reports for them.
- Creation and storage of report data, including financial data for the Client, for the production of a report.
- this operation relates to all aspects of Personal Data processed.
- Technical support, issue diagnosis and error correction to ensure the efficient and proper running of the systems and to identify, analyses and resolve technical issues both generally in the provision of the Services 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.
- Virus, anti-spam and Malware checking in accordance with the Services provided. This operation relates to all aspects of Personal Data processed.
- URL scanning for the purposes of the provision of targeted threat protection and similar service which may be provided under the Agreement. This operation relates to attachments and links in emails and will relates to any Personal Data within those attachments or links which could include all categories of Personal Data.

Exhibit B

Technical and Organizational Security Measures

The Processor utilizes third party data centers to host the Genie9 application and they maintain current ISO 27001 certifications and/or SSAE 16 SOC 1 Type II or SOC 2 Attestation Reports. The Processor will not utilize third party data centers that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations.

Upon the Controller's written request (no more than once in any 12-month period), the Processor shall provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Services). Any audit report submitted to the Controller shall be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties.

The following descriptions provide an overview of the technical and organizational security measures implemented. It should be noted however that, in some circumstances, in order to protect the integrity of the security measures and in the context of data security, detailed descriptions may not be available, however additional information regarding technical and organizational measures may be found in the Security Policy. It's acknowledged and agreed that the Security Policy and the technical and organizational measures described therein will be updated and amended from time to time, at the sole discretion of the Processor. Notwithstanding the foregoing, the technical and organizational measures will not fall short of those measures described in the Security Policy in any material, detrimental way.

1. Entrance Control

The Processor's EU based cloud provider conforms to ISO 27001 certifications and/or SSAE 16 SOC 1 Type II or SOC 2 to ensure secure entrance control.

All offices are locked when unsupervised to prevent unauthorized access to Personal Data.

2. System Access Control

The Processor's EU based cloud provider conforms to ISO 27001 certifications and/or SSAE 16 SOC 1 Type II or SOC 2 to ensure secure system access control.

Following industry best practice the Processor utilizes a centralized, role-based authentication and access system which provides access to all key customer processing systems. This means that passwords are very strong and non-authorized staff do not have knowledge of them. When a staff member leaves, they are simply removed from this system which removes their access from all systems that they were approved to access.

As per best practice all PCs are locked when unattended.

3. Data Access Control

Role based authorization is extensively used throughout the organization, and other applications used for processing Customer Data to implement "need-to-know" principles.

The Processor's database is encrypted "at rest" and in addition implements column level encryption on Personal data.

4. Transmission Control

All Genie9 application transmissions are encrypted.

The Genie9 application is hosted within the EEA.

5. Data Entry Control

Technical and organizational measures regarding recording and monitoring of the circumstances of data entry to enable retroactive review.

System inputs are recorded in the form of log files therefore it is possible to review retroactively whether and by whom Personal Data was entered, altered or deleted.

6. Data Processing Control

Technical and organizational measures to differentiate between the competences of principal and contractor:

The aim of the data processing control is to provide that Personal Data is processed by a commissioned data processor in accordance with the Instructions of the principal. Details regarding data processing control are set forth in the Agreement and the DPA.

7. Availability Control

The Genie9 database is saved in triplicate to ensure availability. In addition, the database is backed up at least every 4 hours and can be restored to at least any 4-hour point in the last 14-day period, using a mechanism of full, differential and database log backups.

8. Separation Control

Technical and organizational measures regarding purposes of collection and separated processing:

- Personal Data is used for internal purposes only e.g. as part of the respective customer relationship, may be transferred to a third party such as a subcontractor, solely under consideration of contractual arrangements and appropriate data protection regulatory requirements.
- Employees are instructed to collect, process and use Personal Data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems.
- Customer Data is stored in a way that logically separates it from other customer's data.
- Genie9 contains security mechanisms to ensure that users only have access to data that they are authorized to access.