Data Processing Agreement

This Data Processing Agreement ("**DPA**"), dated _____ forms part of the Master Services Agreement dated [ ] ("**MSA**") between:

Sentient Solutions Limited (hereinafter referred as **"Sentient")**.

and

[ ] (hereinafter referred as "**Customer**");

This DPA sets out the additional terms, requirements and conditions on which Sentient will process Personal Data when providing its Services to Customer.

The terms used in this DPA shall have the meanings set forth herein. Terms not otherwise defined herein shall have the meaning given to them in the MSA. Except as modified below, the terms of the MSA shall remain in full force and effect.

By entering into the MSA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Legislation, in the name and on behalf of its Affiliates for which Sentient processes Personal Data as Processor.

In the event of conflict between this DPA and the MSA, this DPA shall prevail with respect to the Processing of Personal Data.

AGREED TERMS

1. **Definitions**

All capitalized terms not defined herein shall have the meaning set forth in the MSA. The following additional definitions apply in this DPA.

"CCPA" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).

"**Controller**" means the Customer or the entity, alone or jointly with others, that determines the purposes and means of the Processing of Personal Data.

"**Data Subject**" means an identified or identifiable natural person.

"**Data Protection Legislation**" means (a) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"); (b) the Irish Data Protection Acts 1988 and 2018; (c) the European Communities (Electronic Communications Networks & Services) (Privacy & Electronic Communications) Regulations 2011; (d) the UK GDPR and the UK Data Protection Act 2018; (e) the EU ePrivacy Directive 2002/58/EC (as amended) (the "**ePrivacy Directive**"); and (f) any relevant transposition of, or successor or replacement to the laws detailed at (a) to (e) inclusive, all as amended, re-enacted and/or replaced from time to time, and any other applicable legislation relating to the collection, processing, transfer, or retention of Personal Data.

"Delete" means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed.

"**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a Data Subject.

"**Personal Data Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data processed by Sentient or its Sub-processors.

"Process", "Processed" or "Processing" means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means Sentient or an entity that Processes Personal Data on behalf of the Controller.

"**Sensitive Personal Data**" has the meaning given in Article 9 GDPR.

"**Standard Contractual Clauses**" means the European Union standard contractual clauses for international transfers from the European Economic Area to third countries, Commission Implementing Decision (EU) 2021/914 of 4 June 2021, available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914.

"Sub-processor" means any third party processor engaged by Sentient or its Affiliates engaged in the Processing of Personal Data.

2. INTRODUCTION

2.1 In providing the Services under the MSA, Sentient may be required to process Personal Data on Customer's behalf. The parties acknowledge that Customer acts as Controller and Sentient acts as Processor in respect of Personal Data. The parties shall act reasonably and in good faith in exercising their rights under this DPA.

2.2 Customer (and any Affiliates) shall, at all times, comply with their respective obligations as Controller and shall be responsible for Processing of all Personal Data processed under or in connection with the MSA by their Authorised Users in accordance with their obligations under applicable Data Protection Legislation. Customer shall have sole responsibility for the accuracy, quality, and legality of the Personal Data and the means by which Customer acquires the Personal Data.

2.3 Customer is responsible for ensuring that it has a lawful basis for Processing Personal Data and for providing all required privacy notices to Data Subjects in each case that are necessary for Sentient to Process (and have Processed by Sub-processors) Personal Data under or in connection with this DPA in accordance with Data Protection Legislation. Furthermore, Customer shall not, by act or omission, cause Sentient to violate Data Protection Legislation, as a result of Sentient or its Sub-processors Processing the Personal Data in accordance with this DPA.

2.4 Customer shall not use the Services to process Sensitive Personal Data unless expressly agreed in writing. Customer shall notify Sentient in writing prior to engaging with the Services if the Personal Data includes any of the following: (i) credit, debit or other payment card data subject to the Payment Card Industry Data Security Standards; (ii) patient, medical or other protected health information regulated by the Health Insurance Portability and Accountability Act ("HIPAA"); or (iii) any other personal data of an EU citizen deemed to be in a "special category" (as identified in the GDPR or any successor directive or regulation). Customer acknowledges that Sentient is not a Business Associate or subcontractor (as those terms are defined in

HIPAA) or a payment card processor and that the Services are neither HIPAA nor PCI DSS compliant.

2.5 Schedule 1 to this DPA sets out certain information regarding Sentient and its Sub-processors Processing of the Personal Data.

2.6 Customer hereby instructs Sentient (and consents and authorises Sentient to instruct each Sub-processor) to process Personal Data as reasonably necessary for the provision of the Services.

3. **DATA PROTECTION OBLIGATIONS**

3.1 To the extent that Sentient Processes Personal Data pursuant to the MSA, Sentient shall:

3.1.1 Process Personal Data only on the Customer's documented instructions including as set out in the MSA and this DPA. Sentient shall immediately inform Customer if, in its opinion, an instruction infringes Data Protection Legislation or other data protection provisions;

3.1.2 Process any Personal Data only to the extent required to provide the Services and in accordance with all Data Protection Legislation, unless required to do otherwise by law, in which case, where legally permitted, Sentient shall inform Customer of such legal requirement before Processing;

3.1.3 not Process Personal Data for any purpose other than for the business purposes specified in MSA or otherwise retain, use or disclose Personal Data outside of the direct business relationship between Sentient and Customer;

3.1.4 taking into account the nature and extent of Processing, implement and maintain technical and organizational measures to ensure a level of security appropriate to the risk presented by Processing the Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data Processed.

3.1.5 not permit any Processing of any Personal Data outside of the European Economic Area and/or the United Kingdom without Customer's prior written consent and subject then in any event to the execution of an appropriate data transfer agreement in compliance with Data Protection Legislation in accordance with clause 7, unless Sentient or Sub-processors are required to transfer the Personal Data to comply with applicable laws and such laws prohibit notice to Customer on public interest grounds;

3.1.6 cooperate as reasonably requested by Customer to enable Customer to: (i) comply with any exercise of rights by a Data Subject under the Data Protection Legislation in respect of Personal Data processed by Sentient under this DPA and shall implement and maintain appropriate technical and organisational measures to assist Customer in responding to such requests from Data Subjects and shall notify Customer promptly upon receipt of any such request from a Data Subject. Sentient shall not respond to any request from a Data Subject except on the documented instructions of Customer or as required by law, in which case Sentient shall to the extent permitted by law inform Customer of that legal requirement before Sentient responds to the request;

3.1.7 upon Customer's request, Sentient shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligations under Data

Protection Legislation, including with regards to data privacy impact assessments and consultations with supervisory authorities, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Sentient. Cooperation may include the provision of appropriate technical and organisational measures, where possible, through the Sentient Services and/or as outlined in the User Documentation. Any such reasonable assistance shall be at the cost of Customer;

3.1.8 maintain proper up to date records of any Personal Data Processed by or on behalf of Sentient pursuant to this DPA;

3.1.9 ensure that any person authorized to process the Personal Data: (i) have committed themselves to appropriate contractual confidentiality obligations or are under an appropriate statutory obligation of confidentiality; (ii) Processes the Personal Data solely on behalf and in accordance with the instructions from Customer; and (iii) are appropriately reliable, qualified, and trained in relation to their Processing of Personal Data;

3.1.10 appoint and identify to Customer a named individual within Sentient to act as a point of contact for any enquiries from Customer relating to Personal Data and cooperate in good faith with Customer concerning all such enquires within a reasonable time period; and

3.1.11 upon termination of the MSA and at Customer's written request, Sentient shall delete or return the Personal Data in accordance with the MSA, unless retention is required by law. Return of Personal Data to Customer may be by way of Customer retrieving a final export via Sentient APIs. Sentient shall on request provide a certificate of confirmation from a senior authorised representative of Sentient that this paragraph 3.1.11 has been complied with in full in accordance with Sentient procedures.

4. **PERSONAL DATA BREACH**

4.1 Without prejudice to the other provisions of this DPA, Sentient shall promptly upon becoming aware and in any event within twenty four (24) hours of becoming aware of a Personal Data Breach, notify Customer of the Personal Data Breach where the Personal Data Breach directly affects Personal Data or the Services being offered to Customer.

4.2 Sentient shall, at no additional cost to Customer (save that Customer shall reimburse Sentient's reasonable costs where Sentient has complied fully with its obligations under this DPA and such Personal Data Breach is not due to Sentient default or neglect), provide sufficient information and assistance to Customer in ensuring compliance with its obligations in relation to notification of Personal Data Breaches, and communication of Personal Data Breaches to Data Subjects where the breach is likely to result in a high risk to the rights of such Data Subjects, and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of such Personal Data Breach.

5. **California Consumer Privacy Act ("CCPA")**

5.1 If Sentient is Processing Personal Data within the scope of the CCPA ("CCPA Personal Data") these additional provisions for CCPA Personal Data shall apply only with respect to CCPA Personal Data:

5.1.1 Roles of the Parties. When Processing CCPA Personal Data in accordance with Customer instructions, the parties acknowledge and agree that Customer is a "Business" and Sentient is a "Service Provider" for the purposes of the CCPA.

5.1.2 Responsibilities. The parties agree that Sentient shall Process CCPA Personal Data as a Service Provider strictly for the purpose of performing the Processing activities ("Business Purpose") or as otherwise permitted by the CCPA.

5.1.3 Sentient shall Process Personal Data on behalf of the Customer and not retain, use, or disclose that data for any purpose other than the Business Purpose, as otherwise set out in the MSA or as permitted under the CCPA;

5.1.4 In no event shall Sentient sell, retain, use, or disclose any Personal Data made available by Customer other than for the Business Purpose, as otherwise set out in the MSA or as permitted under the CCPA;

5.1.5 Sentient acknowledges and agrees that it shall comply with its obligations as a Service Provider under the CCPA; and

5.1.6 the parties acknowledge that the CCPA may be amended and agree to comply with such amendments and regulations when they become effective, subject to Sentient's right to terminate the MSA if the CCPA materially impacts the Processing activities or Sentient's rights and obligations under the MSA.

6. SUB-PROCESSORS

6.1 Customer confirms its prior general consent to sub-processing of the Personal Data by Sentient's current Sub-processors, an up to date list of which is maintained by Sentient on its website at https://www.scorebuddyqa.com/security and available on request, and which may be updated in accordance with Clause 6.2. The Sub-processor list shall include the identities of the Sub-processors, their country of location as well as a description of the Processing they perform.

6.2 Sentient shall provide Customer with written notice with sufficient detail of any proposed additional or replacement Sub-processors prior to the introduction of any such addition or replacement. Customer may, acting reasonably, object to any particular proposed Sub-processor on data protection grounds. If no written objections have been received within thirty (30) calendar days of the date of notice, the proposed Sub-processor shall be deemed accepted.

6.3 Sentient shall ensure that: (i) it shall enter into an agreement with the Sub-processor and the terms governing the engagement between Sentient and any Sub-processor are not less protective with respect to Processing of Personal Data compared to the provisions of this DPA and any other relevant provisions of the MSA to the extent those requirements are applicable to the nature of the services provided by the Sub-processor; and (ii) Sentient shall remain responsible and liable for the Sub-processor's compliance with its obligations and for any acts or omissions of such Sub-processor.

7. DATA TRANSFERS

7.1 If Sentient transfers Personal Data outside the EEA or UK to a third country that is not recognized by the European Commission (or relevant authority) as providing an adequate level of protection, such transfers shall be governed by the Standard Contractual Clauses. Where

required under applicable Data Protection Legislation, the Standard Contractual Clauses (including, where applicable, the UK International Data Transfer Addendum) are incorporated by reference into this DPA and shall be deemed entered into and binding on the parties upon the commencement of the relevant restricted transfer. The parties agree that the parties shall comply with the provisions of the applicable Module of the Standard Contractual Clauses specified in Schedule 1 and, with respect to the elements of the Standard Contractual Clauses that require the parties' input, Schedules 1 and 2 contain information relevant to the Standard Contractual Clauses' Annexes. In case of any conflicts or inconsistency between the provisions of this DPA and the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses shall prevail.

7.2 The parties agree that, for Personal Data of Data Subjects in the United Kingdom, they adopt the modifications to the Standard Contractual Clauses listed in Schedule 2 to adapt the Standard Contractual Clauses to local law, as applicable.

7.3 Without limiting the generality of the foregoing, Sentient shall enter into (and shall cause its Sub-processors to enter into) any additional agreements or adhere to any additional contractual terms and conditions related to the Processing, including cross border data transfer, of Personal Data to the extent reasonably required to comply with applicable Data Protection Legislation.

8. **AUDIT**

8.1 Subject to Clause 8.2 and to the extent required by applicable Data Protection Legislation, Customer shall have the right to audit Sentient systems, processes, and procedures relevant to the protection of Personal Data.

8.2 An audit under this Clause 8 shall be: (i) carried out no more than once in any twelve (12) month period during the Term, unless it needs to be carried out more than once a year to comply with a request from an authority or a legal or regulatory obligation on the part of the Controller; (ii) conducted during Business Hours over the course of one Business Day; (iii) subject to a minimum thirty (30) days' prior written notice; and (iv) in relation to the Customer's Personal Data only. Sentient shall grant to Customer (or representatives of Customer that are not competitors of Sentient) a right of access to Sentient's premises and/or systems during Business Hours for the purpose of such audit, and Sentient shall give such necessary assistance to the conduct of such audits.

8.3 Customer shall bear any and all expenses incurred by Sentient in respect of any such audit and any such audit shall not interfere with the normal and efficient operation of Sentient's business. Sentient may require, as a condition of granting such access, that Customer (and representatives of Customer) enter into reasonable confidentiality undertakings with Sentient. The parties shall work cooperatively to agree an audit plan, scope and timing in advance of any audit.

8.4 If the scope of the audit is addressed in an ISO 27001/27701 or similar audit report performed by a qualified third party auditor within the previous twelve (12) months, and Sentient data protection or other relevant officer certifies in writing there are no known material changes in the controls audited, Customer shall agree to accept those reports in lieu of requesting an audit of the controls covered by the report. Sentient shall reasonably cooperate with and assist Customer where a Regulator requires an audit of Sentient's Processing of Personal Data in order to ascertain or monitor Customer's compliance with Data Protection Legislation.

9. **INDEMNITY**

The parties shall indemnify each other ("Indemnified Party") from and against third party claims, suits, demands and actions and for resulting damages, awards of damages, losses, costs, and expenses (including but not limited to reasonable legal and professional fees) incurred by a party that result from a breach by either party of the terms and conditions of this DPA and/or Data Protection Legislation. Such breaching party shall be liable on a comparative basis for the portion of those damages directly attributable to its breach of its obligations and the indemnity shall be subject to the limitations of liability in the MSA. If any third party makes a claim against the Indemnified Party, or notifies an intention to make a claim against the Indemnified Party, the Indemnified Party shall: (i) give written notice of the claim against the Indemnified Party to the indemnifying party as soon as reasonably practicable; (ii) not make any admission of liability in relation to the claim against Indemnified Party without the prior written consent of the indemnifying party; (iii) at the indemnifying party's request and expense, allow the indemnifying party to conduct the defence of the claim against the Indemnified Party including settlement; and (iv) at the indemnifying party's expense, co-operate and assist to a reasonable extent with the indemnifying party 's defence of the claim against the Indemnified Party.

10. **CHANGES IN DATA PROTECTION LAWS**

Sentient may propose variations to this DPA which Sentient reasonably considers to be necessary to address the requirements of any Data Protection Legislation. The Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified as soon as is reasonably practicable. Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Sentient to comply with Data Protection Legislation.

11. **TERM AND TERMINATION**

11.1 This DPA is effective automatically upon Customer's acceptance of the MSA and remains in force for the duration of the MSA and any period during which Sentient processes Personal Data on Customer's behalf ("**Term"**).

11.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the MSA in order to protect the Personal Data will remain in full force and effect.

Signed for and on behalf of Sentient Solutions Limited t/a Scorebuddy by its duly authorised representative -

Name:	
Signature:	
Title:	**CEO**
Date:	

Signed for and on behalf of [ ] by its duly authorised representative:

Name:	
Signature:	
Title:	
Date:	

Schedule 1

Details of Processing of Personal Data

(a) Subject matter and duration of the Processing of Personal Data

The subject-matter of the Processing is the Processing of Personal Data by Sentient on behalf of Customer for the purpose of providing the Services under the MSA. The duration of the Processing of Personal Data is set out in the MSA.

(b) The nature and purpose of the Processing of Personal Data

Sentient shall Process Personal Data as necessary to perform the Services pursuant to the MSA and as further instructed by the Customer in its use of the Services.

(c) The types of Personal Data to be Processed

Personal Data relating to the following type of data categories. The types of Personal Data may change from time to time, according to any additional or amended Services to be provided by Sentient.

The data entered into the Scorebuddy platform is at the discretion of the user but would typically include user access account details, attached files from the user environment and basic user information for individuals being assessed.

Should a client choose to enable the Scorebuddy surveys add on module, contact lists of client customers or lists from other sources may be uploaded and stored in the system.

General User
- System ID
- Employee ID
- First name
- Last Name
- Company Email Address

Contact Lists for use with the Surveys Module
- System ID
- First name
- Last Name
- Email Address
- Mobile Number

(d) The categories of Data Subject to whom Personal Data relates

Personal Data relating to the following type of Data Subjects:

- Authorised Users (as defined in the MSA)
- Client customers

(e) The obligations and rights of Customer

These are as set out in the MSA and this DPA.

Sentient may provide notice of change to these provisions where an update is required due to changes to services or changes required due to applicable Data Protection Legislation, including the interpretation thereof.

Schedule 2

Information for International Transfers

Categories of data subjects whose Personal Data is transferred
As described in Schedule 1.

Categories of Personal Data transferred
As described in Schedule 1.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
As described in Schedule 1.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)
Data is transferred on a continuous basis during the term of the MSA, unless otherwise specifically agreed elsewhere between Customer and Sentient.

Nature of the Processing
Sentient shall Process Personal Data as necessary to perform the Services pursuant to the MSA as further instructed by Customer and/or its Affiliates by virtue of using the Services, including storage, organisation, structuring, disclosure by transmission, dissemination or making available, and other forms of Processing.

Purpose(s) of the data transfer and further Processing
To provide the Services to Customer and, as applicable, its Affiliates, as further specified in the MSA.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period
Personal Data will be retained for the duration of the MSA and deleted or returned in accordance with the DPA, unless retention is required by law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the Processing
Sentient uses Sub-processors and will engage Sub-processors solely as necessary to provide the Services to Customer and, as applicable, its Customer Affiliates, and Sub-processors will carry out any Processing of Personal Data only as necessary for such purposes and as further instructed by Customer and/or its Customer Affiliates by virtue of using the Services, including hosting, storage and other forms of Processing. Such Processing will be no longer than for the duration of the MSA, unless otherwise agreed upon in writing.

For the purposes of the Standard Contractual Clauses (Module 2 – Controller to Processor, and Module 3 where applicable):

- Clause 9(a): Option 2 (general written authorisation). Notice period: 30 days.
- Clause 11: The optional independent dispute resolution mechanism does not apply.
- Clause 17: The governing law shall be Ireland.
- Clause 18: The parties submit to the jurisdiction of the courts of Ireland.
- Annex I: As described in Schedule 1.
- Annex II: Technical and organisational measures are set out in Schedule 3.

For transfers of Personal Data subject to the UK GDPR, the parties incorporate the UK International Data Transfer Addendum to the EU Standard Contractual Clauses (version B.1.0) as issued by the UK Information Commissioner ("**Addendum**").

The information required for Part 1 of the Addendum is set out in this Schedule.

The governing law and forum for the purposes of the Addendum shall be England and Wales.