Qpercom Transforming Assessments Empowering Excellence

SCHEDULE 1

SERVICE PROTOCOL

1. **Software: Qpercom Assessment Platform (**http://client.qpercom.com/**)**

Qpercom manages a number of different types of assessment and manages the scoring process of on-site and remote assessment events. Qpercom manages the assessments of candidates to very high standards using multiple assessors, multiple scoresheets and multiple sites functionality, divergence alerts, and last but not least, communicates personal feedback to candidates.

Qpercom Assessment Platform:

- Improves processes for multiple assessment team members by reducing time, improving accuracy and reducing risks of errors in administrative tasks.
- Provides a station countdown timer starting when candidate ID is confirmed
- Provides two-fold warning alert functionality within station countdown timer
- Calculates results automatically
- Provides a warning system when pre-set multi-assessment team list Divergence threshold is exceeded

- Provides a logging system that verifies who makes any change.
- Establishes standard operating procedures for assessment scoring.
- Automates quality assurance processes.
  - Warning system due to multi-assessment team list Divergence threshold.
  - Allows for text messages in cases of Red Flag or Divergence threshold.
  - Automates the provision of feedback to candidates.

Interoperability
Qpercom works on all browsers across all platforms. The system can be used on any computer, laptop, tablet device or mobile device with connection to Wi-Fi or mobile data. Remote assessment participants are required to take a compatibility check to ensure their device camera and microphone, operating system, browser and network are sufficient to participate in a remote assessment event.

Reporting
All assessment data can be viewed on Qpercom via real-time dashboards and more detailed analysis reports are also available on request. Raw data can be exported per

assessment station and per assessment session. Raw data can be downloaded in Excel format for local additional psychometric analysis in SPSS or other statistical software.

Advanced Analysis
Assessment data can be published for further advanced analysis with Borderline Regression Analysis (raw and adjusted pass mark) and the Standard Error of Measurement (SEM) at two confidence intervals (68% or 95%). Advanced analysis outcomes can be published back to your assessment event and station cut-scores adjusted according to the standard setting applied.

Multi-Station Assessment Events are supported by:

- Multiple assessment teams at multiple sites, each assessment team consisting of a number of assessment team members on consecutive sessions over multiple days.
- A set number of assessment stations (ranging from one to ten or more).
- A set number of assessment team members (ranging from two to six and a number of 'shadow' observers).
- Multiple assessment team members score each individual candidate.
- Separate scoresheets for each candidate, pre-populated with candidate information and the assessment to be addressed by each candidate.
- Scores being reviewed throughout the day of the assessment.

Different levels of users

- Senior Administrators (system wide)
- Branch Administrators (assigned branch wide)
- Assessment Administrators (restricted to assigned fields)
- Assessors (restricted to on-site and remote assessment only)
- Actors (restricted to remote assessment only)
- Candidates (restricted to remote assessment only)
- Clinical Leads
- Support Agents

Scoresheet functionality

- Design options for assessment criteria, and response types (e.g. scoring grid, drop-down list, feedback comments box).
- Assigning of a different score sheet to each individual assessment station or each assessment team member.

  - *Multiple score sheets to avoid carry-over effects between candidates, Qpercom supports 'multiple-assessment scoresheet-design' within one station to enable 'swapping between scenarios'.*

- Assigning of different weightings to each scoresheet/station for an assessment event (different weightings are set by the different total mark per scoresheet).
- To assign minimum pass marks to each scoresheet/assessment station.
- To group scoresheets to a particular assessment event (for final score totalling).
  - *scoresheets can be grouped according to competency modelling/framework and can be grouped according to scenarios or station numbers.*
  - *scoresheets can be searched through advanced 'tagging'.*
  - *Items with scoresheets can be linked to a pre-populated 'competency framework'.*
- To save draft scoresheets which are only visible to administrative users for subsequent amendment.
- To clone scoresheets which can be used across multiple assessments on the system.
- To have an inbuilt countdown timer assigned to each scoresheet (with countdown screen alerts), with the ability for an administrator to edit the time per assessment station/scoresheet.
  - *The inbuilt countdown timer can be set twice using two different warnings at two different times during the countdown.*

Network Capacity
Network capacity is unlimited due to scalable dedicated cloud storage and services. Cloud service up-time is 99%.

Online Web Interface
The online web interface allows users:

- To import a CSV list of candidates to the system (to include names, candidate ID, email address).
- To import a CSV list of assessment team members to the system (to include names, assessment teamlist ID, email address).
- To export a CSV list of candidates and their assessment results per assessment.
- To download all data (flat file type) to import into other local system and reporting tools.

Performance during Assessment

Qpercom Assessment Platform:

- Allows administrators to assign multiple assessors to a specific assessment station/scoresheet on specific days and publish.
- Allows changes of assigned assessors between assessment station/scoresheet.
- Allows assessors to sit on assessment teams in different assessment stations during the same day.
- Allows administrators to move candidates to different circuits within an assessment event allowing:
    - Activation of assessment team list accounts and sending of user credentials.
    - Assessors to view individual score sheets for relevant candidates and enter scores/data against each criterion.
    - Candidate name and ID to be displayed on individual score sheets with the option to display just the ID or in an anonymised format.
    - Assessor name and ID to be displayed on individual scoresheets.
    - Assessor to submit completed scoresheets with the ability to amend and re-submit until account expiry. Changes to scores are all logged by the system.
    - User accounts can be locked and associated login credentials shall become invalid.
- Allows creation of PDF versions of the scoresheets with selected score and feedback sections.
- For assessment team list score analysis, analysis for identifying median (min and max) scores, Mean and standard deviations and divergences in individual assessment team member scoring. Divergence can be set within a certain range plus an SMS service in case the divergence is outside the set range.
    - *Divergence threshold functionality currently available on system along with median and SD*
    - *Qualitative scores available in terms of using a Global Rating Score ranging from non-suitable toward excellent.*
    - *Red and/or amber flagging available in terms of a warning when quality of care and patient safety is in danger.*
- Facilitates viewing an assessment team list or candidate submission timestamp
- Allows displaying candidates in score order (e.g. highest to lowest ranked order)

Remote Assessment

Qpercom Assessment Platform:

- Allows the enabling of video stations by activating the remote assessment setting.
- Facilitates configuration of duration and state names (Preview, Preparation, Reading Time, Assessment, Checkpoint, Group Finished, Assessment Finished) for various stages of remote assessment.
- Provides a timebar with active progress bars and a clock for an administrator to coordinate a remote assessment by moving participants through all stages at appropriate times.
- Offers an overview of all rotations for an assessment event and where candidates are at each stage on the Monitor tab.
- Allows administrators to connect via the Watch tab to assessors and/or actors assigned to each station and to connect to candidates individually in their waiting area for ID checks and briefings. This same process can be used by multiple administrators with camera and microphone muted by default for invigilation, proctoring or overseeing purposes.
- Provides the ability to create and send prompts to assessment participants to keep them informed throughout a remote assessment event.
- Reporting facility available to assessment participants to inform administrators of issues that they encounter during an assessment event.
- Media can be attached per role so that assessors, actors and candidates can view PDF and/or video instructions at appropriate times during an assessment event e.g. station instructions for candidates during Reading Time, assessors sharing on demand media during Stations, actors accessing PDF or video instructions in advance of an assessment event, etc…
- Presents phone numbers and email addresses associated with candidate records to allow administrators to contact them outside of Qpercom if they are not logged in for their assessment event.

Online Knowledge Assessment
Qpercom Assessment Platform:

- Allows the authoring of knowledge questions in the Question Bank.
- Facilitates configuration of duration and availability of knowledge assessments so that candidates can access and complete online.
- Reporting facility for online knowledge assessment results and question performance information over multiple assessment events.
- Ability for assessors to score written assessments such as Essay and Short Answer Questions after the fact asynchronously.

Candidate Portfolio
Qpercom Assessment Platform:

- Provides a personal media bank to candidates to upload and curate digital assets.
- Facilitates submission of evidence for verification and feedback from assessors.
- Provides a dashboard showing all upcoming and completed candidate activity as well as learning progress over time.
- Presents all feedback received in a searchable and chronological list to aid learning.

Invigilation/Proctoring
Qpercom Assessment Platform:

- Provides invigilation/proctoring options including record and review and live invigilation.
- Support for Invigilation/proctoring with 2 cameras whereby candidates activate a second camera on their mobile phone via QR code scan on Qpercom.
- Facilitates device lockdown via Safe Exam Browser.

Optional AI-assisted functionality
Qpercom Assessment Platform includes some optional AI-assisted:

- Optional AI-assisted importing of questions or scoresheets in bulk.
- Optional AI-assisted actionable feedback which is shareable with candidates.
- Optional AI-assisted advanced analysis options to query datasets.
- Optional AI-assisted automated proctoring and reporting.

2. **Subscription Term:**

NUMBER OF YEARS for the period COMMENCEMENT DATE to COMPLETION DATE.

3. **Fees & Charges**

3.1 Subscription Fees

Year	**Period**	**Fees & Charges**
Year 1	YEAR DATES	€
Year 2	YEAR DATES	€
Year 3	YEAR DATES	€
Total cost of contract		€

based on NUMBER scoresheets per annum and NUMBER participant video minutes per annum to be used on Qpercom at http://client.qpercom.com/. Fees in subsequent years following the completion of the above period are subject to a Price Indexation adjustment.

3.2 Additional Scoresheets

Scoresheets in excess of the numbers set out in paragraph 3.1 of Schedule 1 must be purchased in blocks of 2,500 Scoresheets, based on the price per Scoresheet within the applicable bundle on Qpercom's Rate Card.

3.3 Additional Remote Assessment Participant Video Minutes

Where remote assessment video is used, participant video minutes in excess of the numbers set out in paragraph 3.1 of Schedule 1 must be purchased based on the applicable price in Qpercom's rate card. Participant video minute fees refer to any user role using an active video tile in live video assessments (e.g. virtual interviews), recorded video (e.g. recorded stations, self-recorded assessments, etc...) and proctoring (e.g. candidate camera and second camera).

All remote assessment participant video minutes and recorded minutes used will be invoiced directly to the client in advance based on an agreed allocation of minutes.

4. Service Availability

The Supplier shall use commercially reasonable endeavours to make the Services available 24 hours a day, seven days a week, except for:

(a) planned maintenance carried out during the maintenance window of Saturday 6.00 am to Sunday 10.00 pm Irish time

(b) unscheduled maintenance performed outside Normal Business Hours, provided that the Supplier has used reasonable endeavours to give the Customer at least six hours' notice in advance.

For the purposes of this Agreement, Normal Business Hours means: 9:00 a.m. to 5:00 p.m. Irish time.

5. Support services:

The Supplier will, as part of the Services and at no additional cost to the Customer, provide the Customer with the Supplier's standard customer support services during Normal Business Hours in accordance with the Supplier's Support Services Policy in effect at the time that the Services are provided. The Supplier may amend the Support Services Policy in its sole and absolute discretion from time to time. The Customer may purchase enhanced support services separately as per Qpercom's rate card.

The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement:

5.1 Service Scope

The following Services are covered by this Agreement;

5.2 Manned telephone support: +35391 395416

- Telephone support : 9:00 A.M. GMT to 5:00 P.M. GMT Monday – Friday on +35391 395416

5.3 Monitored email support and monitored Pubble Instant Messenger:

- Email support: Monitored 9:00 A.M. GMT to 5:00 P.M. GMT Monday – Friday on support@qpercom.ie.
- Emails received outside of office hours will be collected, however no action can be guaranteed until the next working day.
- In application instant messenger support: Monitored 9:00 A.M. GMT to 5:00 P.M. GMT Monday – Friday on support@qpercom.ie.
- Instant messenger support chats received outside of office hours will be collected, however no action can be guaranteed until the next working day.

5.4 Customer Requirements

Customer responsibilities and/or requirements in support of this Agreement include:

- Payment for all support costs at the agreed interval.
- Reasonable availability of customer representative(s) when resolving a service related incident or request.

5.5 Service Provider Requirements

Service Provider responsibilities and/or requirements in support of this Agreement include:

- Meeting response times associated with service related incidents.
- Appropriate notification to Customer for all scheduled maintenance.
- Remote assistance using Remote Desktop and a Virtual Private Network where available.
- Planned or Emergency Onsite assistance (extra costs apply for each site)
- Monthly system health check.

- Nightly server backups are retained for a 2 year period by default. When a retention period is defined by the customer, backups will be deleted in line with the specified retention period.

- Point-in-Time backups are available for a 15 day rolling period where a backup snapshot is taken every 5 minutes. Within the 15 day period, a restoration point can be chosen to restore to should it be required.

5.6 Service Assumptions

Assumptions related to in-scope services and/or components include:

- Changes to services will be communicated and documented to all stakeholders.

5.7 Training

The Customer can avail of 2 hours of remote training per annum where members can learn about the functionality of the system and best practices for using Qpercom for online assessment and analysis.

5.8 Yearly Review Call & Usage Report

The Customer will receive an annual usage report and an end of year review phone call with a representative to discuss usage and ongoing requirements of the system.

5.9 The process of escalation:
In support of services outlined in this Agreement, the Supplier will respond to service related incidents and/or requests submitted by the Customer within the following time frames:

- 0-8 hours (during business hours) for issues classified as High priority.
- Within 48 hours for issues classified as Medium priority.
- Within 5 working days for issues classified as Low priority.

Remote assistance will be provided in-line with the above timescales dependent on the priority of the support request.

6. Social Value, Accessibility & Responsible Innovation

1. Environmental Sustainability & Net Zero

The Supplier shall maintain digital assessment features designed to reduce paper usage and travel emissions associated with physical examinations. The Supplier shall publish and maintain a Carbon Reduction Plan setting out its emissions baseline, reduction targets, and operational progress toward Net Zero.

2. Client Enablement & Educational Development

The Supplier shall provide ongoing support for healthcare education through:

- A live product demonstration accompanying each major platform release;
- Dedicated annual training hours as set out in the Order Form; and
- Access to regular user group sessions, workshops, and webinars to share assessment best practices and product feedback.

3. Accessibility Standards

The Supplier shall maintain a public Accessibility Statement and exercise commercially reasonable efforts to align the SaaS platform with recognized accessibility standards, targeting Web Content Accessibility Guidelines (WCAG) 2.2 Level AA.

4. Responsible Innovation & Supply Chain

Ethical AI & Analytics: Any artificial intelligence or analytics features integrated into the platform shall be developed in accordance with industry-standard security, accessibility, and responsible AI governance principles.

SME Engagement: The Supplier commits to supporting regional economic resilience by prioritizing regional and SME technology partners in its operational supply chain where commercially feasible.

7. Contact Details

Supplier	Address:	Qpercom 9B Galway Technology Centre Platform 94 Mervue Business Park Galway Ireland H91 PY93
	Attn: Telephone: E-mail:	ACCOUNT MANAGER +353 91 395416 support@qpercom.ie
Customer	Address	ADDRESS
	Attn:	CONTACT NAME CONTACT ROLE
	E-mail:	CONTACT EMAIL

DATA PROCESSING AGREEMENT

(A) **DEFINITIONS & INTERPRETATION**

(A) In this Data Processing Agreement ("**DPA**"), unless otherwise defined, all capitalised words and expressions will have the same meanings as are assigned to them in the Software as a Service Subscription Agreement (the "**SAAS Agreement**").

(B) In the event of conflict or inconsistency between this DPA and any of the terms and conditions of the SAAS Agreement, including any in respect of Data Protection Laws, this DPA will be given precedence, unless otherwise set out herein.

(C) If the Customer entity signing the DPA is a party to the SAAS Agreement, the Supplier entity that is party to the SAAS Agreement is a party to this DPA.

(D) If the Customer entity signing this DPA executed orders under the SAAS Agreement but is not a party to the SAAS Agreement, this DPA will be incorporated into such order(s) and the Supplier entity that is a party to such order(s) will be party to this DPA.

(E) This DPA will not be valid and legally binding if the signing Customer entity is not a party to the SAAS Agreement.

(F) In this DPA, the following definitions apply:

SAAS Agreement refers to the Software as a Service Subscription Agreement between the Supplier and the Customer, together with all related and further

agreements and orders executed under it between the Customer and the Supplier.

Alternative Adequate Level of Protection means (i) the country where the Supplier or a Sub-processor is located is recognised by the European Union to have a similar or adequate level of protection of Personal Data as described in Data Protection Laws, or (ii) the Supplier or the Sub-processor has fully implemented binding corporate rules which provide adequate safeguards as required by the Data Protection Laws, or has any other similar program that is recognised as providing an adequate level of protection.

Appropriate Security Measures means appropriate security measures required by Data Protection Laws to protect against unauthorised access to, alteration, disclosure or destruction of data and against their accidental loss or destruction and, in particular, where the processing involves the transmission of data over a network, it shall mean having regard to the state of technological development and the cost of implementing the measures, and ensuring that the measures provide a level of security appropriate to:

the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of or damage to the data concerned, and

the nature of the data.

"Confidential Information" means all information, documents or reports, in whatever form communicated or recorded, relating to the Customer, its business affairs or activities, including but not limited to Data, files, charts, records, lists, payment details and contact information relating to any employee, contractor, player or supporter of the Customer; know-how, formulae, processes, specifications and software programs belonging or relating to the Customer.

Customer means the Customer entity (as identified above) that is a party to the SAAS Agreement and this DPA and who is the Data Controller of the Customer Personal Data.

Customer Group means all companies that are part of the Customer company group.

Customer Personal Data means personal data relating to a living individual who is, or can be, identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Customer and that is provided to the Supplier or collected by

the Supplier from the Customer for the purpose of the Supplier rendering Services to the Customer.

Data Controller means the Customer who, either alone or with others, controls the contents and use of personal data.

Data Processor means any person who processes personal data on behalf of the Data Controller but does not include an employee of the Data Controller who processes such data in the course of his employment.

Data Protection Laws means all legislation and regulations relating to the protection of personal data including (without limitation) the Data Protection Acts 1988 to 2018 of Ireland, the General Data Protection Regulation ("**GDPR**") (when the GDPR comes into force in Ireland) and all other industry guidelines (whether statutory or non-statutory) or codes of practice or guidance issued by the Data Protection Commission or relevant Irish Supervisory Authority (as defined in the GDPR) relating to the processing of personal data or privacy or any amendments and re-enactments thereof.

Data Subject means the person whose Customer Personal Data is, or is to be, Processed.

The Supplier means the Supplier entity (as identified above) that is a party to the SAAS Agreement and this DPA and who is the Data Processor of the Customer Personal Data.

The Supplier Group means all companies that are part of the Supplier company group.

EEA means European Economic Area.

Loss includes any demand, claim, proceeding, suit, judgement, loss, liability, cost, expense, fee, penalty or fine.

Permitted Purpose means the purpose required by the Customer from the performance of the Services by the Supplier or any Specific Request.

Privacy Statement means the Supplier privacy statement located at http://client.qpercom.com/ (as updated from time to time).

Process or Processing means any operation or set of operations which is performed upon Customer Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making

available, alignment or combination, blocking, erasure or destruction. Any derivative of the word **Process** has a corresponding meaning.

Personnel means those employees of the Supplier to whom disclosure of Personal Data is necessary for the provision of services and who are appropriately trained in and committed to data security and confidentiality.

Specific Request means any instruction, in email or other form, to the Supplier stating the specific services that the Customer requires and containing the information required by the Supplier to perform those specific Services

Standard Contractual Clauses means those standard contractual clauses which are pre-approved, model data protection clauses developed by the European Commission to facilitate compliant cross-border data transfers, especially to countries outside the European Economic Area (EEA).

Sub-processor means any Data Processor engaged by the Supplier to perform Services.

(B) **STATUS OF THE PARTIES**

(A) **Status:** The parties acknowledge that, in relation to Customer Personal Data, and for the purposes of the Data Protection Law, the Supplier is a Data Processor.

(B) **Ownership:** As between the Customer (the Data Controller) and the Supplier (the Data Processor), all Customer Personal Data shall at all times be the property of the Customer and/or the Customer's Authorised Users.

(C) **Application of DPA:** The provisions of this DPA shall apply to Customer Personal Data to which the Supplier had access on any date prior to the date of this DPA (the "**Prior Date**") as if this DPA had been executed and come into force on the Prior Date and all Customer Personal Data to which the Supplier has had access since the Prior Date.

(C) **PROVISION OF CUSTOMER PERSONAL DATA**

(A) The Customer will provide Customer Personal Data to the Supplier or the Supplier will collect Customer Personal Data from the Customer and/or the Customer's Authorised Users pursuant to this DPA for the purpose of the Supplier rendering Services to the Customer, or any other members of the Customer Group, and the Supplier will have access to the Customer Personal Data provided by the Customer in the course of rendering the Services.

(B) When the Supplier receives the completed and signed DPA as specified below, this DPA becomes a legally binding addendum to the SAAS Agreement. To make this DPA a part of the SAAS Agreement, the Customer must complete the information in the signature block of this DPA and have an authorised representative sign this DPA.

(D) **USE OF CUSTOMER PERSONAL DATA**

(A) In providing the Services to the Customer pursuant to the SAAS Agreement, the Supplier may Process Customer Personal Data on behalf of the Customer. The Supplier will comply with the provision of this DPA with respect to the Processing of Personal Data provided or collected by and/or on behalf of the Customer using the Services.

(B) The Supplier shall, as instructed by Customer, correct, delete or block the data being Processed under the SAAS Agreement. If an individual should request the correction or deletion of their data, the Supplier shall immediately pass this request to the Customer. Such instruction shall not impact the delivery of the agreed services, and delivery failures caused by such instructions will be the Customer's responsibility.

(E) **RIGHTS AND OBLIGATIONS OF CUSTOMER**

(A) The Customer is the Data Controller of the Customer Personal Data and is responsible for the legitimacy of the Processing of Customer Personal Data and any transfer of Customer Personal Data to a third party. Data Protection Laws determine the rights and obligations of the Customer as a Data Controller as described in this DPA.

(B) As the Data Controller, the Customer shall use its right to issue instructions to the Supplier, as the Data Processor, on the method of Processing Customer Personal Data as well as the services performed by the Supplier. The Customer's submission of Personal Data to the Supplier and instructions for Processing of Personal Data will comply with Data Protection Laws.

(C) The Customer has the right, in relation to Customer Personal Data, to review:

the security measures taken by the Supplier;

the compliance with Data Protection Laws by the Supplier; and

the compliance with this Data Processing Agreement by the Supplier, at any time during normal working days and normal working hours, subject to prior written notice given in advance with a reasonable notice period. The review may take place at the Supplier's place of business by inspecting the stored Customer Personal Data in a storage facility or data centre and the Processing

activities taking place at the premises of the Supplier in accordance with the Supplier's security and access policies.

(D) Data is handled exclusively in accordance with the agreed provisions and in accordance with the Customer's reasonable instructions. Any alterations to the data being Processed and the procedures employed will be discussed, agreed and recorded. The Supplier may supply information to third parties or individuals only if the Customer has given prior written consent.

(E) The Supplier will not use Customer Personal Data for any other purposes, in particular, providing such data to third parties. No copies or duplicates of Customer Personal Data will be made without the Customer's knowledge and agreement, except when copies must be made for security purposes to ensure that data can be preserved in order to comply with legal requirements.

(F) **RIGHTS AND OBLIGATIONS OF THE SUPPLIER**

(A) The Supplier shall only Process Customer Personal Data to the extent necessary pursuant to the Customer's instructions and as set forth in the SAAS Agreement. The Customer instructs the Supplier to Process Customer Personal Data: (i) in accordance with the SAAS Agreement; (ii) as part of any Processing initiated by the Customer in its use of the Services; and (iii) to comply with the Customer's reasonable instructions to the extent they are consistent with the terms of the SAAS Agreement.

(B) The Supplier will conduct the Processing in compliance with Data Protection Laws.

(C) The Supplier shall inform the Customer as soon as practicable if, in its opinion, it receives an instruction from the Customer which infringes Data Protection Law.

(D) The Supplier shall disclose Personal Data only to those members of its Personnel to whom such disclosure is necessary for the exercise of its rights, and performance of its obligations, under this agreement and shall procure that such persons are made aware of, and agree in writing to observe the obligations of confidentiality in clause 8.

(E) The Supplier shall not copy or maintain any Personal Data on any other systems, application or other medium other than as required for the Permitted Purpose.

(F) The Supplier will keep Customer Personal Data confidential and ensure Appropriate Security Measures are in place and take appropriate technical, physical and organisational security measures as described in the Privacy Statement to protect Customer Personal Data against unauthorised or unlawful Processing, accidental loss or damage or destruction.

(G) The Supplier is obliged to provide information and cooperate when the Customer conducts a review as described in Section 5.3; however, the Supplier shall not be required to disclose any commercial or trade secrets (including, without limitation, algorithms, source codes, etc.). The Supplier also will reasonably assist the Customer (at the Customer's expense) in the event of data protection checks or audits by a data protection authority, to the extent that such checks or audits relate to the Processing under this DPA.

(H) All persons under the Supplier's employ or control who can access Customer Personal Data in the course of performing their duties for the Supplier shall be made aware of the obligations to keep the data confidential. The Supplier and the Customer agree to instruct their respective employees on their particular data protection obligations arising from this DPA and the existence of their duty to act as directed or for the purpose stipulated.

(I) The Supplier will promptly inform the Customer of any actual or suspected security breach involving Customer Personal Data. The Supplier must take adequate remedial measures immediately and must promptly provide the Customer with all the relevant information and assistance as reasonably requested by the Customer regarding the actual or suspected security breach.

(J) The Supplier shall inform the Customer as soon as reasonably possible if: (i) a formally designated authority demands the access to Customer Personal Data, or (ii) a formally designated authority has taken measures against the Supplier, unless the Supplier is by law prohibited from informing the Customer about the request of such authority or the measures taken.

(K) The Supplier agrees with the Customer that for the duration of the provision of the Services it shall only process, use and disclose the Customer Personal Data for the Permitted Purpose and strictly in accordance with the instructions of the Data Controller as set out in a Specific Request from time to time and in accordance with the terms of this DPA.

(L) The Supplier agrees with the Customer that for the duration of the provision of the Services it shall not sell, transfer, disclose or allow access to any Customer Personal Data to any other party other than those of its officers, employees, agents and contractors to whom, and to the extent to which, such disclosure is necessary for the Permitted Purpose or in accordance with the express approval of the Customer.

(M) The Supplier agrees with the Customer that for the duration of the provision of the Services, it shall take reasonable steps to ensure that the Customer Personal Data is accurately recorded and kept up to date.

(N) The Supplier agrees with the Customer that for the duration of the provision of the Services, it shall not perform the Services in such a way as to cause the Customer to breach any of its obligations under the Data Protection Laws.

(O) The Supplier shall make available to the Customer all information necessary to demonstrate its compliance with the obligations set out in Data Protection Law and shall allow the Customer access to the Supplier's premises, Personnel and relevant records to the extent necessary to enable it to verify the Supplier's compliance with Data Protection Law and its obligations under this Agreement.

(G) **ADDITIONAL REQUIREMENTS FOR TRANSFER OF PERSONAL DATA OUTSIDE THE EEA**

(A) The Customer acknowledges and agrees that the performance of the Services may involve from time to time, a transfer of Customer Personal Data from the Supplier to Sub-Processors located outside the EEA. In respect of such transfers and where no Alternative Level of Protection applies, the Supplier shall ensure that in addition to the requirements described in Section 6 of this DPA, certain additional requirements shall be met.

(B) The additional requirements which must be met pursuant to Section 7.1 above are incorporated in Standard Contractual Clauses which, where required, must be entered into between the Supplier and a Sub-Processor.

(H) **CONFIDENTIALITY**

(A) **Keep Confidential:** The Supplier shall keep confidential the Confidential Information and shall not, without the prior written consent of the Customer, use, disclose, copy or modify the Confidential Information other than is necessary for the exercise of its rights, and performance of its obligations, under this Agreement.

(I) **SUB-PROCESSORS**

(A) Pursuant to Clause 5(h) of the EU Model Standard Contractual Clauses, the Customer acknowledges and expressly agrees that the Supplier is entitled to retain any member of the Supplier Group ("**the Supplier Affiliates**") as further sub-processors for the Supplier and that the Supplier or the Supplier Affiliates respectively may engage third-party service providers as sub-processors that may provide customer support, including processing of Customer Personal Data, in connection with the Services.

(B) **Sub-processors**. The Supplier, upon prior written request, shall make available to the Customer for the Customer's approval a current list of sub-processors for the Services

with the identities of those Sub-processors ("**Sub-processor List**") (such approval not to be unreasonably delayed or withheld).

(C) **Objection Right for new Sub-processors.** If the Customer has a reasonable basis to object to the Supplier's use of a new Sub-processor, the Customer shall notify the Supplier promptly in writing within 10 business days after receipt of the Supplier's notice. In the event the Customer objects to a new Sub-processor(s) and that objection is not unreasonable, the Supplier will use reasonable efforts to make available to the Customer a change in the affected Services or recommend a commercially reasonable change to the Customer's configuration or use of the affected Services to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If the Supplier is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days, the Customer may terminate the applicable Service(s) in respect only to those Services which cannot be provided by the Supplier without the use of the objected-to new Sub-processor, by providing written notice to the Customer. The Customer shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services.

(D) All Sub-processors will be subject to data protection obligations at least equivalent to those contained in this DPA under a written agreement, and such sub-processors shall be obliged to comply with applicable Data Protection Laws. Where the Sub-processor fails to fulfil its data protection obligations under such written agreement The Supplier shall remain fully liable to the Customer for the performance of the sub-processor's obligations under such agreement.

(E) The Supplier shall audit third-party sub-processors that are not the Supplier Affiliates at least once per year to ensure they have appropriate physical, technical, organisational, and administrative controls in place.

(F) Upon the Customer's prior written request, the Supplier agrees to make available to the Customer a copy of an applicable sub-processor data processing agreement executed in relation to this DPA, provided that the Supplier may remove any commercial information contained in such agreement. The Customer may make available a summary of the agreement, or the agreement if required, to the Customer provided that such summary, or the agreement if required, is treated as Confidential Information, including that the Customer has entered into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the SAAS Agreement to protect the Supplier's Confidential Information.

(J) **SECURITY**

The Supplier shall implement Appropriate Security Measures with a view to preventing accidental or unauthorised, loss, destruction, damage, alteration, disclosure or unlawful or unauthorised access to any Customer Personal Data in the custody of the Supplier, and the Supplier shall procure that its personnel are aware of and comply with those measures.

(K) **BREACH**

(A) **Notice**: The Supplier shall notify all incidents of loss of control of Customer Personal Data to the Customer, as soon as it becomes aware of the incident and in any event no later than 24 hours after so becoming aware.

(B) **Remedy**: In the event of any such breach, the Supplier shall:

take prompt action at its own expense on the instruction of the Customer to remedy the cause of the breach;

bear the costs of investigation into said breach; and

promptly, and at its own expense provide the Customer on request with all information required by the Customer to fulfil its obligations, as data controller, under all applicable laws, regulations and codes of practice.

(L) **DATA SUBJECT REQUESTS**

(A) The Supplier shall promptly notify the Customer of each request from a data subject for access to Customer Personal Data relating to him or her.

(B) The Supplier shall not accede to any such request for access except on the instructions of the Customer (which shall be provided promptly).

(C) The Supplier shall, at the cost and expense of the Customer, upon prior written request by the Customer and taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights under Data Protection Law.

(M) **INDEMNITY**

The Customer shall indemnify the Supplier on demand from time to time from and against all Losses suffered or incurred by the Supplier arising out of or in connection with the breach by the Customer of its obligations under this DPA. The provision of

this Clause shall continue in force and effect without limit in time after the termination of the provision of the Services.

(N) WARRANTIES

The Supplier warrants to the Company that:

- it shall Process the Data with the highest level of care, skill and diligence in accordance with best practice in the Company's industry; and
- its Appropriate Security Measures shall on a continuing basis meet or exceed the requirements of Data Protection Law.

(O) **DURATION**

(A) This DPA will enter into effect on the Effective Date and will remain effective notwithstanding termination of the SAAS Agreement.

(B) Where Customer Personal Data is no longer required by the Supplier for the performance of the Services, the Supplier will either return such data immediately after termination of the SAAS Agreement, or destroy it if requested to do so by the Customer. The Supplier shall certify such destruction or delivery in writing to the Customer upon prior written request from time to time. At such time when Customer Personal Data is either returned or destroyed, this DPA will expire automatically.

(C) To the extent required by applicable Data Protection Laws, this DPA shall be governed by the applicable law of the applicable jurisdiction. In other cases, this DPA will be governed by the laws of the same jurisdiction in the SAAS Agreement.

(D) **Accrued Rights:** The termination of this Agreement shall be without prejudice to the rights of each of the parties accrued up to the termination date.

(E) **Survival of Obligations:** The provisions of Clauses 8, 9, 13, 14 and 15 shall survive the expiry or termination of the Contract and this Agreement however it arises, and shall continue to bind the Contractor.

(P) **CONFLICTING PROVISIONS**

(A) The DPA supersedes any conflicting terms in the SAAS Agreement. Notwithstanding the foregoing, the SAAS Agreement and the terms of this DPA apply only between the parties and do not confer any rights to any third party Data Subjects.

(B) This DPA does not replace any additional rights or obligations related to processing of Customer Data in the SAAS Agreement.

(Q) **NOTICES**

(A) The parties will send any communications or notices required under this DPA in writing, which includes by fax or e-mail, to the following focal points:

- **GenAI Collaboration Opt-In:**

PURPOSE AND CONSENT

Qpercom may invite the client to participate in a GenAI research collaboration aimed at improving the generation of structured, context-aware feedback and enhancing psychometric tools. Participation is entirely optional and will proceed only upon the client's express, written consent. The collaboration will involve analysis of fully anonymised datasets and will not involve any identifiable data.

SAFEGUARDS AND ANONYMISATION

Qpercom commits to implementing strict data governance, including irreversible anonymisation of all research data, limited internal access, and audit logging. No identifiers or linkages will be retained, and re-identification is expressly prohibited. Research results will not be published or externally shared without prior notification to the client.

CLIENT RIGHTS AND IP

The client retains full ownership of all assessment data and any outputs generated through Qpercom's GenAI tools used within the client's environment. Qpercom retains only the right to develop and improve its internal methodologies based on fully anonymised or synthetic data. Any findings may be shared with the client to support local educational improvement at no additional cost.

OPTIONAL INVOLVEMENT

The client may choose to:

- Review research protocols or findings,
- Be acknowledged in relevant academic dissemination,
- Receive updates on research outcomes annually.

WITHDRAWAL AND DURATION

The client may revoke their participation in the collaboration at any time with written notice. Upon withdrawal, Qpercom will cease using the client's data for any further GenAI research activities. This clause remains valid for the duration of the main agreement unless terminated by either party with 60 days notice.

DATA RETENTION

By default, all client data is retained on Qpercom indefinitely giving a historical overview of candidate performance over time. However, should the client wish to enforce a data retention period, you can do so here by specifying how long in years you wish data to remain on Qpercom and what data you want removed on expiry of the data retention period.

Data Retention Period: _____

Data Removal Preference: _____