DATA PROCESSING AGREEMENT

THIS AGREEMENT is made on the [*add date*] day of *[add month year]*

BETWEEN

1.0 The Parties

(herein after called the “Controller”) of the one part and

2.0 Purpose

The Purpose of the processing is described within Schedule A.

This Agreement sets out the terms and conditions under which Data held by the Controller will be disclosed to and used by the Processor.

The Purpose is consistent with the original purpose of the Data creation and/or collection.

The Processing of Data for the Purpose will assist the Controller to fulfil his obligations as described in Schedule A.

Controllership of the Data shall at all times remain with the Controller.

3.0 Definitions

The following words and phrases used in this Agreement shall have the following meanings except where the context otherwise requires:

Purpose means the purpose of the Processing as set out within Schedule A.

Aggregated Data means Data presented to the extent that no living individual can be identified from the Aggregated Data or any other Data in the possession of, or likely to come into the possession of any person obtaining the Aggregated Data.

Data, **Controller**, **Data Subject, Processor**, **Personal Data, Personal Data Breach, Pseudonymisation and Processing**, have the same meaning as in Article 4 of GDPR.

Data Protection Impact Assessment means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Data Protection Legislation means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy and (iii) all applicable Law about the processing of personal data and privacy.

Special Categories of Personal Data has the same meaning as in Article 9 of GDPR.

GDPR means the General Data Protection Regulation (Regulation (EU) 2016/679)

LED means the Law Enforcement Directive (Directive (EU) 2016/680)

Data Loss Event means any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject Access Request means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their personal data.

Data means any Data including Personal Data and Special Categories of Personal Data, to be provided to, or collected by, the Data Processor and processed on behalf of the Controller as identified at **Schedule A**.

Services means the Data Processing activity and services to be undertaken by the Data Processor on behalf of the Controller, as identified in **Schedule A**.

Party means a Party to this Agreement.

Client Manager means the person who has oversight and responsibility for ensuring the Processing on behalf of the Controller or other such person as shall be notified to the Processor from time to time is in compliance with the terms of this Agreement. The Manager will assume responsibility for co-ordinating data protection compliance, notification, security, confidentiality, audit and co-ordination of subject rights and Freedom of Information requests as directed by the terms of this Agreement.

Project Manager means *the person* who has day-to-day management responsibility for the Processing and compliance with this Agreement on behalf of the Processor or such other person as shall be notified to the Controller from time to time. The Project Manager will assume responsibility for data protection compliance, notification, security, confidentiality, audit and co-ordination of subject rights and Freedom of Information requests as directed by the terms of this Agreement.

Protective Measures means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted.

Law means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, by-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply.

Agreement means this Data Processing Agreement together with its schedules and all other documents attached to or referred to as forming part of this Agreement.

Confidential Information means all Data and any other information relating to the Controller's customers and prospective customers, current or projected financial or trading situations, business plans, business strategies, developments and all other information relating to the Controller's business affairs including any trade secrets, know-how and any information of a confidential nature imparted by the Controller to the Processor during the term of this Agreement or coming into existence as a result of the Processor's obligations, whether existing in hard copy form or otherwise, and whether disclosed orally or in writing.

Miscellaneous
Headings are inserted for convenience only and shall not affect the construction or interpretation of this Agreement and, unless otherwise stated, references to clauses and schedules are references to the clauses of and schedules to this Agreement;
Any reference to any enactment or statutory provision shall be deemed to include a reference to such enactment or statute as extended, re-enacted, consolidated, implemented or amended and to any subordinate legislation made under it; and

The word 'including' shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and the word 'include' and its derivatives shall be construed accordingly.

4.0 Provision or collection of Data

The manner and frequency of transmission of Data from the Controller to the Processor is set out in Schedule A.

5.0 Access to the Data

Access to the Data will be restricted to the Controller or those employees of the Processor as identified in Schedule B and authorised by the Controller, directly involved in the processing of the Data in pursuance of the Purpose.

6.0 Data Protection and Human Rights

The processing of any Personal Data shall be in accordance with the obligations imposed upon the Parties to this Agreement by the Data Protection Legislation. All relevant codes of practice or data protection operating rules adopted by the Parties will also reflect the data protection practices of each of the parties to this Agreement.

The Processor shall notify the Controller immediately if it considers that any of the Controllers instructions infringe the Data Protection Legislation.

The only processing that the Processor is authorised to do is listed in Schedule A by the Controller and may not be determined by the Processor. Where deviation from Schedule A is required this will only occur where previously authorised in writing by the Manager to the Project Manager.

The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:
(a) a systematic description of the envisaged processing operations and the purpose of the processing;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
(c) an assessment of the risks to the rights and freedoms of Data Subjects; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

The Processor may not contact any Data Subject except where permitted by Schedule A.

The Processor shall notify the Controller immediately if it:
(a) receives a Data Subject Access Request (or purported Data Subject Access Request);
(b) receives a request to rectify, block or erase any Personal Data;
(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;
or
(f) becomes aware of a Data Loss Event.

The Processor's obligation to notify under the preceding clause shall include the provision of further information to the Controller in phases, as details become available.

Taking into account the nature of the Processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under preceding clauses (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
(a) the Controller with full details and copies of the complaint, communication or request;
(b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
(d) assistance as requested by the Controller following any Data Loss Event;
(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Agreementor employs fewer than 250 staff, unless:

(a) the Controller determines that the processing is not occasional;
(b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
(c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

The Processor shall allow for audits of its Processing activity by the Controller or the Controller's designated auditor.

The Processor shall designate a data protection officer if required by the Data Protection Legislation.

Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:
(a) notify the Controller in writing of the intended Sub-processor and processing;
(b) obtain the written consent of the Controller;
(c) enter into a written Agreement with the Sub-processor which give effect to the terms set out in this Agreement such that they apply to the Sub-processor; and
(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

The Processor shall remain fully liable for all acts or omissions of any Sub-processor.

The Processor may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Customer may on not less than 30 Working Days' notice to the Processor amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office

The Parties agree and declare that the information accessed pursuant to this Agreement will be used and processed with regard to the rights and freedoms enshrined within the European Convention on Human Rights. Further, the Parties agree and declare that the provision of information is proportional, having regard to the purposes of the Agreement and the steps taken in respect of maintaining a high degree of security and confidentiality.

If any Party to this Agreement receives a request for information under the provisions of the Freedom of Information Act 2000 identified as originating from another Party, the receiving Party will contact the other Party to determine whether the latter wishes to claim an exemption under the provisions of that Act.

Where the Data Processor receives a request for information under the provisions of the Freedom of Information Act 2000 in respect of information provided by or relating to the Controller, the Processor will contact the Manager to ascertain whether the Controller wishes to claim any exemption including the determination of whether or not the

Controller wishes to issue a response neither to confirm nor deny that information is held.

7.0 Confidentiality

The Data Processor shall not use or divulge or communicate to any person (other than those whose province it is to know the same for the Purpose, or without the prior written authority of the Controller) any Data obtained from or created on behalf of the Controller, which it shall treat as private and confidential and safeguard accordingly[1]
The Data Processor shall ensure that any individuals who process Data under this Agreement are aware of their responsibilities in connection with the use of that Data and have confirmed so in writing by completion of Annex C: Undertaking of Confidentiality which will be provided to the Manager as a pre-requisite for that individual to process Data.

For the avoidance of doubt, the obligations or the confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement .

Respect for the privacy and rights of Data Subjects will be afforded at all stages of the Purpose.

The restrictions contained within this section shall cease to apply to any Data which may come into the public domain otherwise than through unauthorised disclosure by the Parties to the Agreement.

8.0 Retention, Review and Deletion

The Data will be retained by the Processor and then securely disposed by the Processor in accordance with Schedule A.

9.0 Security

Description	Details
Subject matter of the processing	*The generation of bias test scores and feedback reports*
Duration of the processing	*Processing within 72 hours. Data deleted after 120 days.*

[1] The restriction set out in this paragraph shall not apply where disclosure of the Data is ordered by a Court of competent jurisdiction, or subject to any exemption under the Data Protection Act 2018, where disclosure is required by a law enforcement agency or regulatory body or authority, or is required for the purposes of legal proceedings, in which case the Processor shall immediately notify the Controller in writing of any such requirement for disclosure of the Data in order to allow the Controller to make representations to the person or body making the requirement.

Nature and purposes of the processing	*The generation of psychometric tests scores and the creation of automated feedback reports. The administration of tests results.* Group level data (no identified personal data) retained without limit to report group and sector data.
Type of Personal Data	*Name, Email. Bias test scores.* *In some use scenarios may include Age, Ethnicity, Sexual Orientation, Religion/Faith, Gender and Disability status and a range of other differences*
Categories of Data Subject	*Test takers from across client organisations* *Research subjects.*
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	*Retained for a maximum of 120 days. Destruction sequenced after 90 days.*
GDPR Officer	*Dr Pete Jones*

The Data Processor recognises that the Controller has obligations relating to the security of Data in his control under the Data Protection Legislation, ISO7799 and the ACPO Information Community Security Policy. The Processor will continue to apply those relevant obligations as detailed below on behalf of the Controller during the term of this Agreement.

The Data Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with Schedule A, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Customer before processing the Personal Data unless prohibited by Law;
(b) ensure that it has in place Protective Measures, which have been reviewed and approved by the Controller as appropriate to protect against a Data Loss Event having taken account of the:
(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;
(c) ensure that:
(i) employees of the Processor do not process Personal Data except in accordance with this Agreement (and in particular Schedule A);
(ii) it takes all reasonable steps to ensure the reliability and integrity of any employees who have access to the Personal Data and ensure that they:
(A) are aware of and comply with the Processor's duties under this clause;
(B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and
(D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
(d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Customer;
(ii) the Data Subject has enforceable rights and effective legal remedies;
(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Processor on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.

The Controller may wish to undertake suitability checks (including vetting) on any persons having access to premises and the Data and further reserves the right to issue instructions that particular individuals shall not be able to participate in the Purpose without reasons being given for this decision. The Processor will ensure that each person who will participate in the Purpose understands this and provides their written consent as necessary.

10.0 Disputes

In the event of any dispute or difference arising between the Parties out of this Agreement, the Designated Manager and the Project Manager or the persons appointed pursuant to this Agreement shall meet in an effort to resolve the dispute or difference in good faith.

The Parties will, with the help of the Centre for Dispute Resolution, seek to resolve disputes between them by alternative dispute resolution. If the Parties fail to agree within 56 days of the initiation of the alternative dispute resolution procedure, then the Parties shall be at liberty to commence litigation.

11.0 Term, Termination and Variation

The Controller may at any time by notice in writing terminate this Agreement/ Agreement forthwith if the Data Processor is in material breach of any obligation under this Agreement.

At the discretion of the Controller this Agreement/ Agreement shall terminate after the replacement of the Project Manager.

Either Party may terminate this Agreement/ Agreement by giving 30 days notice in writing to the other Party.

The Controller will have the final decision on any proposed variation to this Agreement/ Agreement. No variation of the Agreement/ Agreement shall be effective unless it is contained in a written instrument signed by both Parties and annexed to this Agreement/ Agreement

12.0 Miscellaneous

This Agreement acts in fulfilment of part of the responsibilities of the Controller as required by Articles 28 and 29 and Recital 81 of GDPR.

This Agreement constitutes the entire agreement between the Parties as regards the subject matter hereof and supercedes all prior oral or written Agreement regarding such subject matter.

Or

This Agreement compliments the Call Off/ Procurement Agreement between the Parties.

If any provision of this Agreement is held by a Court of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect the remaining provisions of this Agreement, which shall remain in full force and effect.

The validity, construction and interpretation of the Agreement and any determination of the performance which it requires shall be governed by the Laws of England and Wales and the Parties hereby submit to the exclusive jurisdiction of the English Courts.

Signed on behalf of the Client

.....

.....

Signed on behalf of Bias Test

.....

.....

Schedule A: Details of Data to be provided to, or collected by, the Processor and processed on behalf of the Controller.

The Processor shall comply with any further written instructions with respect to processing from the Controller.

Any such further instructions shall be incorporated into this schedule.

Schedule B: Details of employees of the Processor authorised to have access to and otherwise process the Data

Annex A: Security Report

Should the Processor or any Sub-Processor incur a Data Loss Event with the personal data belonging to the Controller. Within 24 hours of the Data Loss Event becoming known, the Processor shall report it to the Controller by completing the form below and sending it to: client email address

Incident Date: Time:
Reporting Organisation:
Reporting Date: Time:
Reported by (Name & Job title):
Contact Telephone Number:
Email Address:
Incident location:

Incident details and actions taken (please provide as much information as you can to ease the handling of the incident):

Please give as much description of the nature of the personal data breach including number of individuals concerned:

Categories (eg staff, victims, suspects, convicted) and approx. number of people concerned:

Categories and approx. number of personal data records concerned:

Section 2 Information Security Organisation
Responsibility for information security should be allocated to an individual within the organisation.

That individual should be operating within a management framework that initiates and controls the implementation of information security.

Please advise who has designated responsibility for information security within your organisation and describe their role and the management framework within which they operate

Dr Pete Jones

Section 3 Assets Classification and Control
It is important to maintain appropriate protection of the computer and information assets used by the data processor.

Please list below the hardware, software and information, which will be used for the purposes of the Agreement*.*

Thinkpad. Flash.

What accountability for these assets is in place? Who will be the nominated System Owner of these assets for the purpose of the Agreement*?*

Dr Pete Jones

Section 4 Personnel Security

How has the reliability of persons subject to this Agreement *been assessed?*

Only company director has access. Underwent police security clearance following work with British Transport Police

Any persons having access to data as part of this Agreement *may be required to give consent to background enquiries in accordance with Force policy. Please provide written consent as required.*

Agreed.

Please confirm that all persons connected with this project have received training and awareness in Data Protection and information security. A confidentiality clause will be included in the Agreement which all persons involved may be required to sign.

Yes

Please confirm that all persons involved with this project are made aware of the procedure for reporting any security breaches, threats, weaknesses of malfunctions that might impact on the security of the data.

Yes

Section 5 Physical and Environmental Security
Appropriate measures should be in place to prevent unauthorised access or unlawful processing, accidental loss, destruction or damage.

Please advise details of the premises used for this purpose and in relation to each named premises:-

a) What access controls are there to the buildings?	*Lap tops are routinely used in a range of locations to access the web site/server where data is held. There is no physical location other than the sever where data is held.*
b) What access controls are there to the rooms?	*NA*
c) Are the windows lockable when accessible from the outside?	*NA*
d) Is the door lockable where the information is stored?	*NA*
e) Is information secured in a lockable cabinet when not in use?	*NA*
f) Is there a clear desk policy in relation to this information?	*NA*
g) Do outside Agreementors/maintenance/cleaning staff have access to the room?	*NO*
h) Is the information visible to unauthorised individuals, i.e., through windows, from corridors etc.	*No*

i) Is there any intention to use portable computers for this purpose? If so, what special control measures will be deployed to protect data?	*Lap top protected by password and access to server by a further log in and password. System security tested by penetration testing by https://www.sec-1.com/*
j) Is the computer/server used to store data in connection with the project physically secured in any way (e.g. by cable to desk etc.)?	*No data storage on site.*

Section 6 Computer and Network Management

In addition to the physical security outlined above, please provide details of the following:-

a) Is the computer a stand-alone? If not, What measures are taken to prevent unauthorised access via your network or from external networks?	*Lap top protected by password and access to server by a further log in and password. System security tested by penetration testing by https://www.sec-1.com/*
b) Is there a policy and procedure for the disposal of sensitive material (computer or otherwise)? What procedure is in place to ensure that the data is cleansed from computer media as it becomes obsolete for whatever reason? What procedure is in place to ensure that data held on computer media is handled appropriately when equipment is sent for repair?	*No data held on lap top.*
c) Are system security procedures regularly audited?	*Lap top protected by password and access to server by a further log in and password. System security tested by penetration testing by https://www.sec-1.com/*
d) Are there documented rules for the use of this system available for all users? If so, do users sign to show they have read and understood the Rules?	*Policy attached.*
e) What control measures are in place to prevent the introduction of malicious software to the system (e.g., computer viruses)?	*Lap top protected by password and access to server by a further log in and password. System security tested by penetration testing by https://www.sec-1.com/ Server security detail here:* https://www.ionos.co.uk/help/data-protection/overview-of-the-general-data-protection-regulation-gdpr/ Agreement-for-data-processing/ https://www.ionos.co.uk/help/fileadmin/pdf/en_GB/Datenschutz/Customer_DPA_UK.pdf

Section 7 System Access Controls

a) Are there controls on the system to prevent unauthorised access (i.e. Is there a mechanism for the identification and authorisation of individual users, e.g., user ID and password)?	*Only one admin password issued, known to only one person. System security both admin and user password and log in systems tested by penetration testing by https://www.sec-1.com/*
b) Is there an automatic log-out after an appropriate time interval?	*Yes*
c) Is there a warning at log-on to forbid unauthorised use of the system?	*No*
d) Is there an audit trail to identify who has accessed the system including time, date and which records were accessed?	*Yes*
e) Who monitors the audit trails? How long are they retained and how is the security of the audit trails maintained?	*Our web designer Mustbebuilt . Retained indefinitely.*

Section 8 Systems Development and Maintenance
All information systems used as part of this Agreement should be designed from the outset with information security in mind to cover, as a minimum, the control measures contained in this document.

Section 9 Business Continuity Planning

a) Is there an effective backup and recovery mechanism to secure the data? And, where is this held?	https://www.ionos.co.uk/help/data-protection/overview-of-the-general-data-protection-regulation-gdpr/ Agreement-for-data-processing/ https://www.ionos.co.uk/help/fileadmin/pdf/en_GB/Datenschutz/Customer_DPA_UK.pdf
b) What security surrounds these	https://www.ionos.co.uk/help/data-protection/overview-of-the-general-data-protection-regulation-gdpr/ Agreement-for-data-processing/

backup facilities?	https://www.ionos.co.uk/help/fileadmin/pdf/en_GB/Datenschutz/Customer_DPA_UK.pdf

Annex C: Undertaking of Confidentiality

Undertaking of Confidentiality

I …….. as an employee of the Processor as defined in the Agreement between the (client name) and Bias Test to which this Undertaking is appended, hereby acknowledge the responsibilities arising from this Agreement.

I understand that my part in fulfilling the Purpose means that I may have access to the Data and that such access shall include

- reading or viewing of information held on computer or displayed by some other electronic means,
- reading or viewing manually held information in written, printed or photographic form, or
- overhearing any radio, telephone or verbal communication.

I undertake that;-

- I shall not communicate to nor discuss with any other person the contents of the Data except to those persons authorised by the Controller as is necessary to progress the agreed Purpose.
- I shall not retain, extract, copy or in any way use any Data to which I have been afforded access during the course of my duties for any other purpose.
- I will only operate computer applications or manual systems that I have been trained to use. This training will include the requirements of the Data Protection Legislation which prescribes the way in which personal data may be obtained, stored and processed.
- I will comply with the appropriate physical and system security procedures made known to me by the Processor.
- I will act only under instruction from the Manager or other relevant official in the processing of any Data.

I understand that the Data is subject to the provisions of the Data Protection Act 2018 and that by knowingly or recklessly acting outside the scope of this Agreement I may incur criminal and/or civil liabilities.

I undertake to seek advice and guidance from the Manager or other relevant official of the Controller in the event that I have any doubts or concerns about my responsibilities or the authorised use of the Data defined in the Agreement.

I have read, understood and accept the above.

Name .....

Signature .....

Date .....