PROCESSOR AGREEMENT is dated dd/mm/yyyy

PARTIES

(1) {Your business name} incorporated and registered in England and Wales with company number {input} whose registered office is at {your registered address} (Controller) (2) (Name of Business) registered in the UK whose address is

BACKGROUND

(A) The Controller and the Processor entered into a SERVICES AGREEMENT that may require the Processor to process Personal Data on behalf of the Controller.

(B) This Personal Data Processing Agreement (Agreement) sets out the additional terms, requirements, and conditions on which the Processor will process Personal Data when providing services under the Services Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation ((EU) 2016/679) for

contracts between controllers and processors.

AGREED TERMS

1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Business Purposes: the services described in the Services Agreement or any other purpose specifically identified in Schedule A.

Data Subject: an individual who is the subject of Personal Data.

Personal Data: means any information relating to an identified or identifiable natural person that is processed by the Processor as a result of, or in connection with, the provision of the services under the Services Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name,

identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing, processes, and process: either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes, or process. It includes any operation or set of operations which is 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. Processing also includes transferring Personal Data to third parties.

Data Protection Legislation: all applicable privacy and data protection laws including the General Data Protection Regulation ((EU) 2016/679) and any applicable national implementing laws, regulations and secondary legislation in England and Wales relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Standard Contractual Clauses (SCC): the European Commission’s Standard Contractual Clauses for the transfer of

Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Schedule to Commission Decision 2010/87/EU, a completed copy of which comprises Schedule B.

1.2 This Agreement is subject to the terms of the Services Agreement and is incorporated into the Services Agreement.

Interpretations and defined terms set forth in the Services Agreement apply to the interpretation of this Agreement.

1.3 The Schedules form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.

1.4 A reference to writing or written includes email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Agreement and any provision contained in the Schedules, the provision in the body of this Agreement will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Schedules, the provision contained in the Schedules will prevail;

(c) any of the provisions of this Agreement and the provisions of the Services Agreement, the provisions of this Agreement will prevail; and

(d) any of the provisions of this Agreement and any executed SCC, the provisions of the executed SCC will prevail.

2. PERSONAL DATA TYPES AND PROCESSING PURPOSES

2.1 The Controller and the Processor acknowledge that for the purpose of the Data Protection Legislation, the Controller is the controller and the Processor is the processor.

2.2 The Controller retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Processor.

2.3 Schedule A describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which the Processor may process to fulfil the Business Purposes of the Services Agreement.

3. PROCESSOR’S OBLIGATIONS

3.1 The Processor will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Controller’s written instructions. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation.

3.2 The Processor must promptly comply with any Controller request or instruction requiring the Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Processor will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Controller or this Agreement specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires the Processor to process or disclose Personal Data, the Processor must first inform the Controller of the legal or regulatory requirement and give the Controller an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 Taking into account the nature of the Processor’s processing, the Processor will assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller’s compliance obligations under the Data Protection Legislation, taking into account and the information available to the Processor, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

4. PROCESSOR’S EMPLOYEES

4.1 The Processor will ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use

restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and

(c) are aware both of the Processor’s duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

4.2 The Processor will take reasonable steps to ensure the reliability, integrity and trustworthiness of all of the Processor’s employees with access to the Personal Data.

5. SECURITY

5.1 The Processor must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in Schedule C.

5.2 The Processor must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of security measures.

6. PERSONAL DATA BREACH

6.1 The Processor will promptly and without undue delay notify the Controller if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. The Processor will restore such Personal Data at its own expense.

6.2 The Processor will immediately notify the Controller if it becomes aware of:

(a) any accidental, unauthorised or unlawful processing of the Personal Data; or

(b) any Personal Data Breach.

6.3 Where the Processor becomes aware of (a) and/or (b) above, it shall, without undue delay, also provide the Controller with the following information:

(a) description of the nature of (a) and/or (b), including the categories and approximate number of both Data Subjects and Personal Data records concerned;

(b) the likely consequences; and

(c) description of the measures taken, or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.

6.4 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. The Processor will reasonably co-operate with the Controller in the

Controller’s handling of the matter, including:

(a) assisting with any investigation;

(b) providing the Controller with physical access to any facilities and operations affected;

(c) facilitating interviews with the Processor’s employees, former employees and others involved in the matter;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Controller; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.

6.5 The Processor will not inform any third party of any Personal Data Breach without first obtaining the Controller’s prior written consent, except when required to do so by law.

6.6 The Processor agrees that the Controller has the sole right to determine:

(a) whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Controller’s discretion, including the contents and

delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.7 The Processor will cover all reasonable expenses associated with the performance of the obligations under clause 6.2 and clause 6.4 unless the matter arose from the Controller’s specific instructions, negligence, wilful default or breach of this Agreement, in which case the Controller will cover all reasonable expenses.

6.8 The Processor will also reimburse the Controller for actual reasonable expenses that the Controller incurs when responding to a Personal Data Breach to the extent that the Processor caused such a Personal Data Breach, including all costs of notice and any remedy as set out in clause 6.6 .

7. CROSS-BORDER TRANSFERS OF PERSONAL DATA

7.1 The Processor (or any subcontractor) must not transfer or otherwise process Personal Data outside the European Economic Area (EEA) without obtaining the Controller’s prior written consent.

7.2 Where such consent is granted, the Processor may only process, or permit the processing, of Personal Data outside the EEA under the following conditions:

(a) the Processor is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. The Processor must identify in Schedule A the territory that is subject to such an adequacy finding; or

(b) the Processor participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Processor (and, where appropriate, the Controller) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the General Data Protection Regulation ((EU) 2016/679). The Processor must identify in Schedule A the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and the Processor must immediately inform the Controller of any

change to that status; or

(c) the transfer otherwise complies with the Data Protection Legislation for the reasons set out in Schedule A.

7.3 If any Personal Data transfer between the Controller and the Processor requires execution of SCC in order to comply with the Data Protection Legislation (where the Controller is the entity exporting Personal Data to the Processor outside the EEA), the parties will complete all relevant details in, and execute, the SCC contained in Schedule B, and take all other actions required to legitimise the transfer.

8. SUBCONTRACTORS

8.1 The Processor may only authorise a third party (subcontractor) to process the Personal Data if:

(a) the Controller provides prior written consent prior to the appointment of each subcontractor; and

(b) the Processor enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Controller’s written request, provides the Controller with copies of such contracts; and

(c) the Processor maintains control over all Personal Data it entrusts to the subcontractor; and

(d) the subcontractor’s contract terminates automatically on termination of this Agreement for any reason.

8.3 Those subcontractors approved as at the commencement of this Agreement are as set out in Schedule A. The Processor must list all approved subcontractors in Schedule A and include any subcontractor’s name and location and contact information for the person responsible for privacy and data protection compliance.

8.4 Where the subcontractor fails to fulfil its obligations under such written agreement, the Processor remains fully liable to the Controller for the subcontractor’s performance of its agreement obligations.

8.5 The Parties consider the Processor to control any Personal Data controlled by or in the possession of its subcontractors.

8.6 On the Controller’s written request, the Processor will audit a subcontractor’s compliance with its obligations regarding the Controller’s Personal Data and provide the Controller with the audit results.

9. COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD PARTY RIGHTS

9.1 The Processor must, at no additional cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Controller as the Controller may reasonably require, to enable the Controller to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of

personal data; and

(b) information or assessment notices served on the Controller by any supervisory authority under the Data Protection Legislation.

9.2 The Processor must notify the Controller immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party’s compliance with the Data Protection Legislation.

9.3 The Processor must notify the Controller within 3 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

9.4 The Processor will give the Controller its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Processor must not disclose the Personal Data to any Data Subject or to a third party other than at the Controller’s request or instruction, as provided for in this Agreement or as required by law.

10. TERM AND TERMINATION

10.1 This Agreement will remain in full force and effect so long as:

(a) the Services Agreement remains in effect, or

(b) the Processor retains any Personal Data related to the Services Agreement in its possession or control (Term).

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

10.3 The Processor’s failure to comply with the terms of this Agreement is a material breach of the Services Agreement. In such event, the Controller may terminate the Services Agreement effective immediately on written notice to the Processor without further liability or obligation.

10.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Services Agreement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within one month, they may terminate the Services Agreement on written notice to the other party.

11. DATA RETURN AND DESTRUCTION

11.1 At the Controller’s request, the Processor will give the Controller a copy of or access to all or part of the Controller’s Personal Data in its possession or control in the format and on the media reasonably specified by the Controller.

11.2 On termination of the Services Agreement for any reason or expiry of its term, the Processor will securely delete or destroy or, if directed in writing by the Controller, return and not retain, all or any Personal Data related to this Agreement in its possession or control. The Processor must enquire of the Controller whether the Controller wants the Personal Data to be

deleted, destroyed, returned or retained.

11.3 If any law, regulation, or government or regulatory body requires the Processor to retain any documents or materials that the Processor would otherwise be required to return or destroy, it will notify the Controller in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

11.4 The Processor will certify in writing that it has destroyed the Personal Data within 3 days after it completes the destruction.

12. RECORDS

12.1 The Processor will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Controller, including but not limited to, the access, control and security of the Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of personal data to a third

country and related safeguards, and a general description of the technical and organisational security measures referred to in

clause 5.1 (Records).

12.2 The Processor will ensure that the Records are sufficient to enable the Controller to verify the Processor’s compliance with its obligations under this Agreement and the Processor will provide the Controller with copies of the Records upon request.

12.3 The Controller and the Processor must review the information listed in the Schedules to this Agreement once a year to confirm its current accuracy and update it when required to reflect current practices.

13. AUDIT

13.1 The Processor will permit the Controller and its third-party representatives to audit the Processor’s compliance with its Agreement obligations. The Processor will give the Controller and its third-party representatives all necessary assistance to conduct such audits. The assistance may include, but is not limited to:

(a) physical access to, remote electronic access to, and copies of the Records and any other information held at the Processor’s premises or on systems storing Personal Data;

(b) access to and meetings with any of the Processor’s personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c) inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data.

13.2 The notice requirements in clause 13.1 will not apply if the Controller reasonably believes that a Personal Data Breach occurred or is occurring, or the Processor is in breach of any of its obligations under this Agreement or any Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or the Processor becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, the Processor will:

(a) promptly conduct its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

(c) provide the Controller with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within 7 days.

13.4 At the Controller’s written request, the Processor will:

(a) conduct an information security audit before it first begins processing any Personal Data and repeat that audit on an annual basis;

(b) produce a written report that includes detailed plans to remedy any security deficiencies identified by the audit;

(c) provide the Controller with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within 7 days.

14. WARRANTIES

14.1 The Processor warrants and represents that:

(a) its employees, subcontractors, agents and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation relating to the Personal Data;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Services Agreement’s contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in clause 5.1.

14.2 The Controller warrants and represents that the Processor’s expected use of the Personal Data for the Business

Purposes and as specifically instructed by the Controller will comply with the Data Protection Legislation.

15. INDEMNIFICATION

15.1 The Processor agrees to indemnify, keep indemnified and defend at its own expense the Controller against all costs, claims, damages or expenses incurred by the Controller or for which the Controller may become liable due to any failure by the Processor or its employees, subcontractors or agents to comply with any of its obligations under this Agreement or the

Data Protection Legislation.

15.2 Any limitation of liability set forth in the Services Agreement will not apply to this Agreement’s indemnity or reimbursement obligations.

16. NOTICE

16.1 Any notice or other communication given to a party under or in connection with this Agreement must be in writing and delivered to:

For the Controller: {your name } at email {your email address}

For the Processor: (name) at email

16.2 Clause 16.1 does not apply to the service of any proceedings or other documents in any legal action or, where

applicable, any arbitration or other method of dispute resolution.

17. No private work of the category 'business improvement' may be undertaken with any data subject for the duration of this service agreement.

This agreement has been entered into on the date stated at the beginning of it.

Signed by {your name}

for and on behalf of {your business}

Signed by (name of person)

for and on behalf of (name of Business)