Data Processing Agreement: Within the UK and UK to EEA (Controller-to-Processor)

PARTIES

The Client: the party requesting supply of the Services as specified in the Master Agreement (Client)

The Supplier: Bluecrest Health Screening Ltd incorporated and registered in England and Wales with company number 08119445 whose registered office is at Ridgeworth House, 5/9 Liverpool Gardens, Worthing, England, BN11 1RY (Supplier)

BACKGROUND

The Client and the Supplier entered into a contract for the provision of private health assessments (Master Agreement) that may require the Supplier to process Personal Data on behalf of the Client.

This Personal Data Processing Agreement (Agreement) sets out the additional terms, requirements, and conditions on which the Supplier will process Personal Data when providing services under the Master Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors.

AGREED TERMS

1. Definitions and Interpretation

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

Authorised Persons: the persons or categories of persons that the Client authorises to give the Supplier written personal data processing instructions as identified in Annex A and from whom the Supplier agrees solely to accept such instructions.

Business Purposes: the services to be provided by the Supplier to the Client as described in the Master Agreement and any other purpose specifically identified in Annex A.

Commissioner: the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing: have the meanings given to them in the Data Protection Legislation.

Controller: has the meaning given to it in section 6, DPA 2018.

Data Protection Legislation:

a) To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of Personal Data.

b) To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which the Client or Supplier is subject, which relates to the protection of Personal Data.

Data Subject: the identified or identifiable living individual to whom the Personal Data relates.

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

EEA: the European Economic Area.

Personal Data: means any information relating to an identified or identifiable living individual that is processed by the Supplier on behalf of the Client as a result of, or in connection with, the provision of the services under the Master Agreement; an identifiable living individual 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 the individual.

Processing, processes, processed, process: any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.

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

Processor: a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller.

Records: has the meaning given to it in Clause 12.

Services: as specified in the Master Agreement.

Term: this Agreement's term as defined in Clause 10.

UK GDPR: has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2. This Agreement is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this Agreement.

1.3. The Annexes 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 Annexes.

1.4. A reference to writing or written includes faxes and 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

Annexes, 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 Annexes, the provision contained in the Annexes will prevail; and

(c) any of the provisions of this Agreement and the provisions of the Master Agreement, the provisions of this Agreement will prevail.

2. Personal data types and processing purposes

2.1. The Client and the Supplier agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Client is the Controller and the Supplier is the Processor.

(b) the Client retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Supplier.

(c) Annex A describes the subject matter, duration, nature, and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Supplier may process the Personal Data to fulfil the Business Purposes.

3. Supplier's obligations

3.1. The Supplier 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 Client's written instructions. The Supplier 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. The Supplier must promptly notify the Client if, in its opinion, the Client's instructions do not comply with the Data Protection Legislation.

3.2. The Supplier must comply promptly with any Client written instructions requiring the Supplier to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3. The Supplier will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third-parties unless the Client or this Agreement specifically authorises the disclosure, or as required by domestic or EU law, court or regulator (including the Commissioner). If a domestic or EU law, court, or regulator (including the Commissioner) requires the Supplier to process or disclose the Personal Data to a third-party, the Supplier must first inform the Client of such legal or regulatory requirement and give the Client an opportunity to object or challenge the requirement, unless the domestic or EU law prohibits the giving of such notice.

3.4. The Supplier will reasonably assist the Client, at no additional cost to the Client, with meeting the Client's compliance obligations under the Data Protection Legislation, taking into account the nature of the Supplier's processing and the information available to the Supplier, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation.

3.5. The Supplier must notify the Client promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Supplier's performance of the Master Agreement or this Agreement.

4. Supplier's employees

4.1. The Supplier will ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

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

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

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

5. Security

5.1. The Supplier must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the 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 Annex B. The Supplier must document those measures in writing and periodically review them at least annually to ensure they remain current and complete.

5.2. The Supplier 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 the security measures.

6. Personal data breach

6.1. The Supplier will within 48 hours and in any event without undue delay notify the Client in writing if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Supplier will restore such Personal Data at its own expense as soon as possible.

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

(c) any Personal Data Breach.

6.2. Where the Supplier becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Client with the following written information:

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

(b) the likely consequences; and

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

6.3. Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Supplier will reasonably co-operate with the Client at no additional cost to the Client, in the Client's handling of the matter, including but not limited to:

(a) assisting with any investigation;

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

(c) facilitating interviews with the Supplier's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(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 Client; and

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

6.4. The Supplier will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Client's written consent, except when required to do so by domestic or EU law.

6.5. The Supplier agrees that the Client has the sole right to determine:

(a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Client'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.

6.6. The Supplier will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 unless the matter arose from the Client's specific written instructions, negligence, wilful default or breach of this Agreement, in which case the Client will cover all reasonable expenses.

6.7. The Supplier will also reimburse the Client for actual reasonable expenses that the Client incurs when responding to an incident of accidental, unauthorised or unlawful processing and/or a Personal Data Breach to the extent that the Supplier caused such, including all costs of notice and any remedy as set out in clause 6.5.

7. Cross-border transfers of personal data

7.1. The Supplier (and any subcontractor) must not transfer or otherwise process the Personal Data outside the UK or, the EEA without obtaining the Client's prior written consent.

8. Subcontractors

8.1. The Supplier may not authorise any third party or subcontractor to process the Personal Data.

8.2. Other than those subcontractors as set out in Annex A, the Supplier may not authorise any other third-party or subcontractor to process the Personal Data.

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

8.4. Where the subcontractor fails to fulfil its obligations under the written agreement with the Supplier which contains terms substantially the same as those set out in this Agreement, the Supplier remains fully liable to the Client for the subcontractor's performance of its agreement obligations.

8.5. The Parties agree that the Supplier will be deemed by them to control legally any Personal Data controlled practically by or in the possession of its subcontractors.

9. Complaints, data subject requests and third-party rights

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

(a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port 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 Client by the Commissioner or other relevant regulator under the Data Protection Legislation.

9.2. The Supplier must notify the Client immediately in writing 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 Supplier must notify the Client 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 other rights under the Data Protection Legislation.

9.4. The Supplier will give the Client, at no additional cost to the Client, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5. The Supplier must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Client's written instructions, or as required by domestic or EU law.

10. Term and termination

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

(a) the Master Agreement remains in effect; or

(b) the Supplier retains any of the Personal Data related to the Master 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 Master Agreement in order to protect the Personal Data will remain in full force and effect.

10.3. The Supplier's failure to comply with the terms of this Agreement is a material breach of the Master Agreement. In such event, the Client may terminate any part of the Master Agreement involving the processing of the Personal Data effective immediately on written notice to the Supplier without further liability or obligation of the Client.

10.4. If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties may agree to suspend the processing of the 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 30 days, either party may terminate the Master Agreement on not less than 30 days on written notice to the other party.

11. Data return and destruction

11.1. At the Client's request, the Supplier will give the Customer, or a third-party nominated in writing by the Client, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Client.

11.2. On termination of the Master Agreement for any reason or expiry of its term, the Supplier will securely delete or destroy or, if directed in writing by the Client, return and not retain, all or any of the Personal Data related to this Agreement in its possession or control.

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

11.4. The Supplier will certify in writing to the Client that it has deleted or destroyed the Personal Data within 10 working days after it completes the deletion or destruction.

12. Records

12.1. The Supplier will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 5.1.

12.2. The Supplier will ensure that the Records are sufficient to enable the Client to verify the Supplier's compliance with its obligations under this Agreement and the Data Protection Legislation and the Supplier will provide the Client with copies of the Records upon request.

12.3. The Client and the Supplier must review the information listed in the Annexes to this Agreement at least once a year to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1. At least once a year, the Supplier will conduct site audits of its Personal Data processing practices and the information technology and information

security controls for all facilities and systems used in complying with its obligations under this Agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.

13.2. On the Client's written request, the Supplier will make summary documentation on all the relevant audit reports available to the Client for review, including as applicable: third-party vulnerability assessments, and reports relating to its ISO/IEC 27001 certification. The Supplier will redact and summarise information in these reports, as deemed appropriate to protect its confidential information and maintain business information security standards. The Client will treat such audit reports as the Supplier's confidential information under the Master Agreement.

13.3. The Supplier will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Supplier's management.

14. Warranties

14.1. The Supplier warrants and represents that:

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

(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 Master 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 accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to, the Personal Data, and ensure a level of security appropriate to:

14.1.d.1. the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage;

14.1.d.2. the nature of the Personal Data protected; and

14.1.d.3. 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 Client warrants and represents that the Supplier's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Client will comply with the Data Protection Legislation.

15. Indemnification

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

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

16. Notice

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

(a) For the Client: the Key Contact email address, as stated in the Master Agreement.

(b) For the Supplier: corporate@bluecrestwellness.com

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.

This Agreement has been entered into on the commencement date of the Master Agreement.

Annex A: Personal Data processing purposes and details

Subject matter of processing:

The Personal Data of eligible persons, as specified by the Client, processed by the Supplier on behalf of the Client as the data controller.

Duration of Processing:

Aligned to the duration of the Master Agreement.

Nature of Processing:

Collection, recording, organisation, structuring, storage, validation, restriction, and destruction (whether or not by automated means) as necessary to provide the Services as described in the Master Agreement.

Business Purposes:

the processing of eligibility to data to provide welcome and booking invitations to the Services the services to be provided by the Supplier to the Client as described in the Master Agreement;

Personal Data Categories:

Full name

Title

Address and Postcode

Gender

Email address

Date of birth

Phone number

Data Subject Types:

Client employees and/or friends and family, as specified in the Master Agreement.

Authorised Persons:

The Key Contact, or contacts authorised by the Key Contact, as specified in the Master Agreement.

Approved Subcontractors:

No subcontractors are involved in the processing of eligibility list data.

Annex B: Security measures

The Supplier will maintain appropriate technical and organisational data security measures. These include:

(a) Physical access controls.

(b) System access controls.

(c) Data access controls.

(d) Transmission controls.

(e) Input controls.

(f) Data backups.

(g) Data segregation.

(h) Employee vetting.

(i) Employee training.