DATA PROCESSING AGREEMENT

between

Edgecumbe Doctor 360 Clients – NHS Trusts or GP Practices

and

Edgecumbe Consulting Group Ltd

CONTENTS

CLAUSE

ANNEX

PARTIES

(1) Edgecumbe Doctor 360 Clients – NHS Organisations, GP Practices **(Customer)**

(2) Edgecumbe Consulting Group Ltd incorporated and registered in England and Wales with company number 3033236 whose registered office is at Whitefriars, Lewins Mead, Bristol, BS1 2NT **(Provider)**

(a) Edgecumbe's ICO registration number is Z7461289

BACKGROUND

(A) The Customer and the Provider entered into a service provider agreement **(Master Agreement)** when purchasing Edgecumbe Doctor 360 Licenses that may require the Provider to process Personal Data on behalf of the Customer.

(B) This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which the Provider 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*) (UK GDPR) 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:

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

Business Purposes: the services to be provided by the Provider to the Customer 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: has the meaning given to it in section 6, DPA 2018.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and the guidance and codes of practice issued by the Commissioner and which are applicable to a party.

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

EEA: the European Economic Area.

Personal Data: means any information relating to an identified or identifiable living individual that is processed by the Provider on behalf of the Customer 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.

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 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 Customer and the Provider agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller and the Provider is the Processor.

(b) the Customer 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 Provider.

(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 Provider may process the Personal Data to fulfil the Business Purposes.

3. Provider's obligations

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

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

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

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

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

4. Provider's employees

4.1 The Provider 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 Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

4.2 The Provider will take reasonable steps to ensure the reliability, integrity and trustworthiness of [and conduct background checks consistent with applicable domestic law on] all of the Provider's employees with access to the Personal Data.

5. Security

5.1 The Provider 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 0. The Provider must document those measures in writing and periodically review them at least annually to ensure they remain current and complete.

5.2 The Provider 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 Provider will promptly and in any event without undue delay notify the Customer 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 Provider 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 Provider becomes aware of (a), (b) and/or (c) above, it will, without undue delay, also provide the Customer 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 Provider will reasonably co-operate with the Customer at no additional cost to the Customer, in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;

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

(c) facilitating interviews with the Provider'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 Customer; 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 Provider 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 Customer's written consent, except when required to do so by domestic law.

6.5 The Provider agrees that the Customer 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 Customer'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 Provider 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 Customer's specific written instructions, negligence, wilful default or breach of this Agreement, in which case the Customer will cover all reasonable expenses.

6.7 The Provider will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to an incident of accidental, unauthorised or unlawful processing and/or a Personal Data Breach to the extent that the Provider 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 Provider (and any subcontractor) must not transfer or otherwise process the Personal Data outside the UK or, the EEA without obtaining the Customer's prior written consent.

8. Subcontractors

8.1 The Provider confirms that its approved subcontractors are under written obligations which contain terms substantially the same as those set out in this Agreement. At the Customer’s reasonable request the Provider agrees to liaise with its subcontractors for the purposes of assuring privacy and data protection compliance.

8.2 Where the subcontractor fails to fulfil its obligations under the written agreement with the Provider, the Provider remains fully liable to the Customer for the subcontractor's performance of its obligations.

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

8.4 On the Customer's written request, the Provider will audit a subcontractor's compliance with its obligations regarding the Personal Data and provide the Customer with the audit results.

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

9.1 The Provider must, at no additional cost to the Customer, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer 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 Customer by the Commissioner under the Data Protection Legislation.

9.2 The Provider must notify the Customer 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 Provider must notify the Customer 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 Provider will give the Customer, at no additional cost to the Customer, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Provider must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Customer's written instructions, or as required by domestic 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 Provider 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 Provider's failure to comply with the terms of this Agreement is a material breach of the Master Agreement. In such event, the Customer may terminate the Master Agreement **OR** any part of the Master Agreement involving the processing of the Personal Data effective immediately on written notice to the Provider without further liability or obligation of the Customer.

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 working days on written notice to the other party.

11. Data return and destruction

11.1 At the Customer's request, the Provider will give the Customer, or a third-party nominated in writing by the Customer, 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 Customer.

11.2 On termination of the Master Agreement for any reason or expiry of its term, if requested to do so the Provider will securely delete or destroy or, if directed in writing by the Customer, 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 Provider to retain any documents, materials or Personal Data that the Provider would otherwise be required to return or destroy, it will notify the Customer 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 Provider will certify in writing to the Customer that it has deleted or destroyed the Personal Data within 30 days after it completes the deletion or destruction.

12. Records

12.1 The Provider 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 (**Records**).

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

12.3 The Customer and the Provider 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 The Provider will permit the Customer and its third-party representatives to audit the Provider's compliance with its Agreement obligations, on at least 7days' notice, during the Term. The Provider will give the Customer and its third-party representatives all necessary assistance to conduct such audits at no additional cost to the Customer. 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 Provider's premises or on systems storing the Personal Data;

(b) access to and meetings with any of the Provider'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 process the Personal Data.

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

13.3 If a Personal Data Breach occurs or is occurring, or the Provider becomes aware of a breach of any of its obligations under this Agreement or any of the Data Protection Legislation, the Provider 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 Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within 30 days.

13.4 At the Customer's written request, the Provider will:

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

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

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

(d) remedy any deficiencies identified by the audit within 30 days.

13.5 At least once a year, the Provider 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.

13.6 On the Customer's written request, the Provider will make all of the relevant audit reports available to the Customer for review. The Customer will treat such audit reports as the Provider's confidential information under the Master Agreement.

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

14. Warranties

14.1 The Provider warrants and represents that:

(a) its employees, subcontractors, 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:

(i) the harm that might result from such accidental, unauthorised or unlawful processing and loss 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 Customer warrants and represents that the Provider's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

15. Indemnification

15.1 The Provider agrees to indemnify, keep indemnified and defend at its own expense the Customer against all costs, claims, damages or expenses incurred by the Customer or for which the Customer may become liable due to any failure by the Provider 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 or other communication given to a party under or in connection with this Agreement must be in writing and delivered to:

For the Customer: The Provider's point of contact with the NHS Trust or GP Practice given when setting up the Doctor 360 licenses for the customer.

For the Provider: Johannah Palmer - Data Protection Officer *gdpr@edgecumbe.co.uk*

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 date the Customer purchased Doctor 360 licenses from the Provider

Signed by Jon Cowell

for and on behalf of Edgecumbe Consulting Group Ltd **(Provider)** Director

ANNEX A Personal Data processing purposes and details

Subject matter of processing: NHS Trusts, GP Practices or Private Medical Organisations require 360 colleague and patient feedback exercises for a specified number of doctors for the purpose of revalidation.

Duration of Processing: for the duration of the master services agreement

Nature of Processing: Includes collecting, recording, organising, structuring, storing, adapting, retrieving, consulting, disclosing by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of data for the following purposes.

Business Purposes: 1) To provide access to doctor 360 questionnaires to Individuals, NHS Trusts, GP Practices or Private Medical Organisations to help participants complete their revalidation process. 2) Clients, doctors and non-clinical staff use Edgecumbe's online portal to set up their doctor 360 exercise, nominate colleagues and / or patients to provide feedback. When the required minimum number of feedback responses are received a report can be generated and downloaded from the portal. Based in the UK.

Personal Data Categories:

Personal Data: Name, email address, postal address, GMC number, profession (GP, Hospital consultant etc.), specialty, place of qualification, year of qualification, age, sex.

Sensitive Personal Data: Ethnic origin, feedback comments (whilst not always sensitive, we cannot predict what a colleague/patient will write)

Data Subject Types: Clients, doctors and non-clinical staff either taking part in a doctor 360 exercise or acting as the revalidation administrators/managers on behalf of their NHS Trust/GP Practice/Private Medical Organisation

Authorised Persons: The Provider's point of contact with the NHS Trust, GP Practice or Private Medical Organisation given when setting up the doctor 360 exercise for the customer.

Approved Subcontractors:

James Massey Design (JMD) Ltd, 1 Sheffield Stables, Southborough, Tunbridge Wells, Kent, TN4 0PD, UK

ROLE: JMD take overall responsibility for the delivery of services and are a specialist design and development company responsible for the design, build and maintenance of the code and hardware that runs the 360° feedback tool, as well as the service provider of the 360° feedback tool which is a brief survey completed by the participant, their boss, peers and direct report team about an individual's behaviour and performance. JMD outsource specialist hosting services to Heart Internet Limited.

We have a DPA in place with JMD

Heart Internet Limited, Units 4 - 5 Tristram Centre, Brown Lane West, Leeds, England, LS12 6BF

ROLE: Heart Internet Limited is a datacenter based in the UK and provides all the hardware, networking and internet connectivity for the service.

SMPT2GO, EPIC Centre, 96-106 Manchester Street, Christchurch 8011, New Zealand

ROLE: SMTP2GO is our outgoing email delivery service that delivers all 360 emails from the 360 systems. Data is held in EU data center.

We have a DPA in place with SMPT2GO.

Microsoft Azure, UK

ROLE: Microsoft Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers. Edgecumbe servers are held in the Microsoft Azure cloud environment. Microsoft Azure data centers are in the UK, a specific location is not provided for security.

Smart Computers IT Support, 20 Apex Court, Woodlands, Bradley Stoke, Bristol, BS32 4JT, UK

ROLE: Edgecumbe's IT support contractor

We have a DPA in place with Smart Computers IT Support

Acronis, Rheinweg 9, Schaffhausen, Switzerland 8200

ROLE**:** Acronis is a cloud back up hosting solution used by our IT Support company where all Edgecumbe data is backed up, data is stored in a UK datacentre. Acronis is ISO27001 accredited. All data within the hosting solution is held in encrypted format, Acronis have no access to data in its unencrypted format.

Provider's security measures

- Physical access controls: all data processed via our sub processors is stored within secure data centres, Edgecumbe is situated within a building manned with 24-hour security; our office has electronic access control. All electronic data is held in the cloud, so no physical server exists. All visitors are managed according to a secure process (access control lists, advanced registration, escorting, sign-in/out, etc.)

- System access controls. Edgecumbe network perimeter is protected by a business grade firewall, all non-essential inbound network ports have been blocked, all essential inbound network ports have been documented and are reviewed on an annual basis or as changes are required., traffic to inbound network ports is monitored and logged using the firewall, a vulnerability scan is performed on the firewall on a quarterly basis or as changes are required.

- Data access controls: Access to all key business applications is governed with unique usernames and password conforming to Edgecumbe's Strong Password Policy, access to data, system utilities and program source libraries is controlled and restricted to those authorised users who have a legitimate business need e.g., systems or database administrators.

- Data backups: All business-critical data is held in the cloud and protected by a separate cloud backup service; The back-up Schedule is as follows:

    - Backed up three times a day
    - Week 1 – Intra-dailies
    - Week 2 – Dailies
    - Week 3 to 6 – Weeklies
    - Week 6+ - Monthlies

- Data segregation: Access to data and network resources is granted to Security Groups rather than to named individuals, staff must be added to Security Groups relevant to their role in the business to gain access to these data and resources.