DATA PROCESSING AGREEMENT

radar healthcare

Date Published: 13th August 2024

This DPA is entered into between Radar Healthcare (a trading name of Smartgate Solutions Limited) and the Customer and is incorporated into and governed by the terms of the Agreement.

1. Definitions

Any capitalised terms not defined in this DPA shall have the meaning given to it in the Agreement.

"**Affiliates**" means any entity that directly or indirectly controls, is controlled by or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party;

"**Agreement**" means the agreement between the Company and the Customer for the provision of the Services;

"**Controller**" means the Customer;

"**Data Protection Legislation**" means all applicable data protection and privacy legislation, regulations and guidance including:

(i) Regulation (EU) 2016/679) (as incorporated into UK legislation by way of the European Union (Withdrawal Agreement) Act 2020 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit)Regulations 2020, together forming the **"UKGDPR"**) and the Privacy and Electronic Communications (EC Directive)Regulations 2003;

(ii) the Data Protection Act 2018; and

(iii) all applicable law about the processing of Personal Data and privacy;

and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data.

"**Data Subject**" shall have the same meaning as in the Data Protection Legislation;

"**DPA**" means this data processing agreement together with Appendix A;

"**Personal Data**" shall have the same meaning as in the Data Protection Legislation;

"**Process**" has the meaning set out in the Data Protection Legislation. 'Processed' and "**Processing**" shall be interpreted in the same way.

"**Processor**" means the Company;

"**Regulator**" means the UK Information Commissioner(including any successor or replacement body);

"**Technical Assurance Document**" means the Company's technicaldocument as updated from time to time, and made reasonably available by the Company;

"**Standard Contractual Clauses**" means the standard clauses for transfers of personal data to third countries adopted under Decision 2021/914 or such other equivalent mechanism adopted by the Regulator pursuant to section 119A of the Data Protection Act 2018;

"**Sub-Processor**" means any person or entity engaged by the Company or its Affiliate to process Personal Data in the provision of the Services to the Customer.

2. Purpose

2.1 The Processor has agreed to provide the Services to the Controller in accordance with the terms of the Agreement. In providing the Services, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

3. Scope

3.1 In providing the Services to the Controller pursuant to the terms of the Agreement, the Processor shall process Personal Data only to the extent necessary to provide the Services in accordance with both the terms of the Agreement and the Controller's instructions documented in the Agreement and this DPA.

4. Processor Obligations

4.1 The Processor may collect, process or use Personal Data only within the scope of this DPA, as further specified in Appendix A.

4.2 The Processor confirms that it shall process Personal Data on behalf of the Controller and shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data shall only process the Personal Data on the documented instructions of the Controller.

4.3 The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breach the Data Protection Legislation.

4.4 The Processor shall ensure that all employees, agents, officers and contractors involved in the Processing of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii)

have received appropriate training on the Data Protection Legislation; and (iii) are bound by the terms of this DPA.

4.5 The Processor shall implement appropriate technical and organisational procedures to protect Personal Data as required by Article 32 of the UK GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

4.6 The technical and organisational measures detailed in the Technical Assurance Document (https://radarhealthcare.com/customer-resources/) shall be at all times adhered to as a minimum security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA.

4.7 The Controller acknowledges and agrees that, in the course of providing the Services to the Controller, it may be necessary for the Processor to access the Personal Data to respond to any technical problems or Controller queries and to ensure the proper working of the Services. All such access by the Processor will be limited to those purposes.

4.8 Personal Data will not be transferred outside of the UK or EEA unless one of the following applies:

(i) the provisions of the Standard Contractual Clauses;

(ii) the third country or territory has been recognised by the Regulator to have an adequate level of protection;

(iii) the organisation is located in a country which has other legally recognised appropriate safeguards in place, such as Binding Corporate Rules; or

(iv) the processing is otherwise necessary for the performance of contract with, or concluded in the interests of, the data subject.

4.9 Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller’s compliance with the Controller’s data protection obligations in respect of the processing of Personal Data.

4.10 The Processor confirms that it and/or its Affiliate(s) have appointed a data protection officer where such appointment is required by applicable data protection legislation. The appointed data protection officer may be reached at dpo@Radar Healthcare.com.

5. Controller Obligations

5.1 The Controller represents and warrants that it shall comply with the terms of the Agreement, this DPA and all applicable data protection laws.

5.2 The Controller represents and warrants that it has obtained any and all necessary permissions and authorisations necessary to permit the Processor, its Affiliates and Sub-Processors, to execute their rights or perform their obligations under this DPA.

5.3 The Controller is responsible for compliance with all applicable data protection legislation, including requirements with regards to the transfer of Personal Data under this DPA and the Agreement.

5.4 All Affiliates of the Controller who use the Services shall comply with the obligations of the Controller set out in this DPA.

5.5 The Controller shall implement appropriate technical and organisational procedures to protect Personal Data as required by Article 32 of the UK GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

5.6 The Controller shall take steps to ensure that any natural person acting under the authority of the Controller who has access to Personal Data only processes the Personal Data on the documented instructions of the Controller.

5.7 The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after the termination of the Agreement. The Processor will process the request to the extent it is lawful and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.

5.8 The Controller acknowledges and agrees that some instructions from the Controller, including destruction or return of data, assisting with audits, inspections or DPIAs by the Processor, may result in additional fees. In such case, the Processor will notify the Controller of its fees for providing such assistance in advance, unless otherwise agreed.

6. Sub-Processors

6.1 The Controller acknowledges and agrees that: (i) Affiliates of the Processor may be used as Sub-processors; and (ii) the Processor and its Affiliates respectively may engage Sub processors in connection with the provision of the Services.

6.2 All Sub-processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor set out in this DPA.

6.3 Where Sub-processors are located outside of the UK or EEA, the Processor confirms that such personal data will only be transferred to that Sub-processor where one of the scenarios listed at clause 4.8 above applies.

6.4 The Processor shall make available to the Controller the current list of Sub-processors which shall include the identities of Sub-processors and their country of location. During the term of this DPA, the Processor shall provide the Controller with prior notification, via email, of any changes to the list of Sub-processor(s) who may process Personal Data before authorising any new or replacement Sub-processor(s) to process Personal Data in connection with the provision of the Services.

6.5 The Controller may object to the use of a new or replacement Sub-processor, by notifying the Processor promptly in writing within ten (10) Business Days after receipt of the Processor's notice. If the Controller objects to a new or replacement Sub-processor, and that objection is not unreasonable, the Controller may terminate the Agreement or applicable Order Form with respect to those Services which cannot be provided by the Processor without the use of the new or replacement Sub-processor. The Processor will refund the Controller any prepaid fees covering the remainder of the Term of the Agreement (or applicable Order Form) following the effective date of termination with respect to such terminated Services.

7. Liability

7.1 The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.

7.2 The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Agreement.

7.3 The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Controller itself.

7.4 The Controller shall not be entitled to recover more than once in respect of the same claim.

8. Audit

8.1 The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

8.2 Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may conduct a more extensive audit which will be: (i) at the Controller's expense; (ii) limited in scope to matters specific to the Controller and agreed in advance; (iii) carried out during UK business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with the Processor's day-to-day business.

8.3 This clause shall not modify or limit the rights of audit of the Controller, instead, it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

9. Data Breach

9.1 The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data ("Data Breach").

9.2 The Processor will take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Data Breach, and to assist the Controller in meeting the Controller's obligations under applicable law.

10. Compliance, Cooperation and Response

10.1 Pursuant to Article 28(3)(f) of the GDPR, the processor agrees to assist the Controller in fulfilling its obligations related to data protection. Specifically, taking into account the nature of the processing and the information available to the processor, the processor shall:

- Assist the Controller in ensuring the security of personal data.
- Support the Controller in notifying personal data breaches to the Information Commissioner's Office (ICO) as required.
- Assist the Controller in notifying affected data subjects of personal data breaches when necessary.

- Aid the Controller in carrying out Data Protection Impact Assessments (DPIAs) when required.

Support the Controller in consulting the ICO when a DPIA indicates a high risk that cannot be mitigated.

10.2 In the event that the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law. The Controller shall reimburse the Processor for all costs incurred as a result of providing reasonable assistance in dealing with a Data Subject request. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable.

10.3 The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller unless such notification is not permitted under applicable law or relevant court order.

10.4 The Processor may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.

10.5 The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a supervisory data protection authority in the performance of their respective obligations under this DPA.

11. Term and Termination

11.1 The Processor will only process Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically 30 days after the expiry of the Agreement.

11.2 The Processor shall at the choice of the Controller, upon receipt of a request received within 30 days at the end of the provision of the Services relating to processing sent to support@RadarHealthcare.com delete or return Personal Data to the Controller. The Processor shall in any event delete all copies of Personal Data in its systems within 60 days of the effective date of termination of the Agreement unless: (i) applicable law or regulations require storage of the Personal Data after termination; or (ii) partial personal data of the Customer is stored in backups, then such personal data shall be deleted from backups up 30 days after the effective date of termination of the Agreement.

12. General

12.1 This DPA sets out the entire understanding of the parties with regard to the subject matter herein.

12.2 Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed upon which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

12.3 This DPA shall be governed by the laws of England and Wales. The courts of England shall have jurisdiction for the settlement of all disputes arising under this DPA.

The parties agree that this DPA is incorporated into and governed by the terms of the Agreement.

Appendix A

You can access information regarding processing activities and technical security measures through the following link.

https://radarhealthcare.com/customer-resources/

Overview of data processing activities to be performed by the Processor

1. The Controller transfers Personal Data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below. The Controller is the Customer.
2. The Processor received data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below.
3. The Personal Data transferred includes but is not limited to the following categories of Data Subjects:

- Employees, freelancers, contractors of the Controller. and other users added by the Controller from time to time.
- Other individuals to the extent identifiable in the content of emails or their attachments or in archiving content. Patients/Residents/Service users whose data is entered during the period of the agreement that the controller utilises the system.
- Authorised Users, Affiliates and other participants from time to time to whom the Controller has granted the right to access the Services in accordance with the terms of the Agreement.
- Clients of the Controller and individuals with whom those end users communicate with by email and/or instant messaging.
- Service providers of the Controller.

4. Categories of Data. The Personal Data transferred includes but is not limited to the following categories of data:

- Personal details, names, user names, passwords, email addresses of Authorised Users.
- Personal Data derived from the Authorised Users use of the Services such as professional information including but not limited to grade, medical speciality,

GMC number and business intelligence information, details relating to patients/residents.

- Personal Data within the email and messaging content which identifies or may reasonably be used to identify, data subjects.
- Metadata including sent, to, from, date, time, subject, which may include Personal Data.
- Photos.
- Data concerning education and profession
- Medical data.
- Criminal convictions records (DBS)
- Workplace related information: company, location, start and end date of employment and other work-related data.
- File attachments that may contain Personal Data.
- The information offered by users as part of support enquiries.
- The survey, feedback and assessment messages
- Other data added by the Controller from time to time.

5. Special categories of Data. The Personal Data transferred includes but is not limited to the following special categories of data:

- Medical data.
- Criminal convictions records (DBS)

6. Processing operations. The Personal Data transferred will be subject to the following basic processing activities:

- Personal Data will be processed to the extent necessary to provide the Services in accordance with both the Agreement and the Controller's instructions. The Processor processes Personal Data only on behalf of the Controller.
- Processing operations include but are not limited to: management of employees, patients, residents and intermediaries, monitoring of the workplace, client management, training, medical registration details, indemnity information, information required for CQC compliance, appraisals, performance reviews, feedback, objectives and personal development tracking, making comments and updates on these, management of lists of employees, intermediaries and other users, providing support to users and other HR functions for medical employers, etc. this operation relates to all aspects of Personal Data processed.
- Technical support, issue diagnosis and error correction to ensure the efficient and proper running of the systems and to identify, analyse and resolve technical

issues both generally in the provision of the Services and specifically in answer to a Controller query. This operation may relate to all aspects of Personal Data processed but will be limited to metadata where possible.

- Virus, anti-spam and Malware checking in accordance with the Services provided. This operation relates to all aspects of Personal Data processed.
- URL scanning for the purposes of the provision of targeted threat protection and similar service which may be provided under the Agreement. This operation relates to attachments and links in emails and will relates to any Personal Data within those attachments or links which could include all categories of Personal Data.