GDPR Data Processing Policy

The terms used in this Policy shall have the meaning as described in this Policy. Capitalised terms not otherwise defined shall have the meaning as set out in the terms and conditions of supply into which it is seemed incorporated (Principal Agreement) or in the Data Protection Laws (as applicable). Except where the context requires otherwise, in the event of any conflict or inconsistency between this Policy and the **Principal Agreement**, the terms of this Policy shallprevail.

1.1 Definitions

In this Policy:

Controller means Bmeimaging Limited or any Controller Group Member with whom the Processor has contracted

Controller Affiliate means any company under common control with the Controller

Controller Group Member means the Controller or any Controller Affiliate

Controller Personal Data means any Personal Data processed by a Contracted Processor on behalf of a Controller Group Member pursuant to or in connection with the Principal Agreement

Contracted Processor means the Processor or a Sub-Processor appointed by the Processor

Data means all Personal Data and Special Categories of Data (as defined under GDPR) collected, generated or otherwise processed by Supplier as a result of, or in connection with, the provision of the Services.

Data Protection Laws means:

(a) the General Data Protection Regulation (EU Regulation 2016/679) (GDPR) and any legislation which amends, re enacts or replaces it in England and Wales;

(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003, together with any legislation which replaces them; and

(c) any other data protection laws and regulations applicable in England and Wales from time to time.

Data Protection Officer has the meaning given to it under Article 37 of GDPR.

Data Subject(s) means the identified or identifiable living individual(s) to whom the Data relates and who is the subject of such Data.

EEA means the European Economic Area.

Losses means claims, demands, actions, awards, judgments, settlements, costs, expenses, liabilities, damages and losses (including all interest, fines, penalties, management time and legal and other professional costs and expenses).

Personal Data has the meaning given to it under the Data Protection Laws.

Processor means the Supplier providing services to the Controller

Processor Affiliate means any company under common control with the Processor.

Records means the records referred to in Clause 1.7.1.

Sub Processor means any person (including any third party and any Processor Affiliate, but excluding an employee of the Processor or any of its sub-contractors) appointed by or on behalf of the Processor or any Processor Affiliate to process Data on behalf of the Controller or a Controller Group Member in connection with the Principal Agreement.

Supervisory Authority means any data protection authority with jurisdiction over the processing of the Data.

Technical and organisational security measures mean those measures aimed at protecting Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of Data over a network, and against all other unlawful or unnecessarily high-risk forms of processing.

1.2 Data Processing

1.2.1 The Processor shall comply with the requirements of the Data Protection Laws in respect of the activities which are the subject of the Principal Agreement and shall not knowingly do anything or permit anything to be done which might lead to a breach by the Controller of the Data Protection Laws.

1.2.2 The Processor may only process Data to the extent it relates to:

(a) the types of Data;
(b) the categories of Data Subject; and
(c) the nature and purpose of processing, which are necessary for the purpose of the fulfilment and delivery of the obligations of the Processor pursuant to the Principal Agreement.

1.2.3 Without prejudice to Clause 1.2.1 the Processor shall:

(a) process the Data only in accordance with the written instructions of the Controller, unless the Processor is required to process the Data for other reasons under the laws of the United Kingdom or the European Union (or a member state of the European Union) to which the Processor is subject. If the Processor is required to process the Data for these other reasons, it shall inform the Controller before carrying out the processing, unless prohibited by relevant law;

(b) immediately inform the Controller if it believes that the Controller's instructions infringe the Data Protection Laws;

(c) have in place, and maintain throughout the Term at all times in accordance with the then current best industry practice all appropriate technical and organisational security measures against:

(i) unauthorised or unlawful processing, use, access to or theft of the Data; and

(ii) loss or destruction of or damage to the Data,

to ensure that the Processor's processing of the Data is in accordance with the requirements of the Data Protection Laws and protects the rights of the Data Subjects (including, as appropriate, the measures set out in Article 32(1) GDPR). On request the Processor shall provide the Controller with a written description of the security measures being taken at that time (for the avoidance of doubt this should take into account the provisions of appropriate, technical and organisational measures to ensure a level of security equivalent to the risk; Article 32 sub sections (1) (a) to (d) provides a non-exhaustive list for consideration);

(d) ensure that all persons authorised by the Processor to process Data are bound by obligations equivalent to those set out in the Confidentiality clause in the Principal Agreement and this Clause 1;

(e) ensure that access to the Data is limited to: 1.2.4 The Processor shall provide such assistance as the Controller requires in order for the

(i) those of the Processor's personnel who need access to the Data to meet the Processor's obligations under the Principal Agreement or this Policy; and

(ii) in the case of any access by any of the Processor's personnel, such part or parts of the Data as is strictly necessary for performance of their duties;

(f) where the Processor is not established in the EU, nominate a representative based in the European Union or the United Kingdom, to the extent required for the Processor to comply with the Data Protection Laws; and

(g) if required under the Data Protection Laws, appoint a Data Protection Officer.

(a) respond to requests relating to the Controller's data processing from Data Subjects;

(b) ensure compliance with the Controller's obligations under the Data Protection Laws, including in relation to:

(i) the security of processing; and

(ii) with the preparation of any necessary data protection impact assessments and the undertaking of any necessary data protection consultations.

1.2.5 The Processor shall take all reasonable steps to ensure the reliability and the trustworthiness of any agent, employee, contractor or such other personnel working on or behalf of the Processor who may have access to any Data the Processor is processing on behalf of the Controller or any Controller Group Member. The Processor shall ensure that access to the Data is only available to those who need to access it and strictly within the terms of this Policy and/or the Principal Agreement.

1.3 Transfers Outside of the EEA

1.3.1 The Processor shall not allow any Data to be processed or transferred to any country outside of the EEA other than to the UK unless:

(a) it notifies the Controller in writing that it intends to transfer any Data outside of the EEA other than to the UK;

(b) the Controller provides its written consent to such transfer (which consent it may give or withhold in its absolute discretion); and

(c) it provides in advance of a transfer authorised under Clause 1.3.1(b) evidence to the Controller's satisfaction of appropriate safeguards, as required by Data Protection Laws.

1.3.2 Failure to comply with this Clause 1.3 shall be deemed an irremediable material breach of contract

1.4 Sub Processors

1.4.1 The Processor shall not engage any Sub-Processor without the Controller's prior written consent. In order to inform the Controller's decision about whether to give or withhold such consent, the Processor shall give to the Controller prior written notice of the appointment of any Sub-Processor, providing full details of the processing to be undertaken, the names of those involved in the sub-processing activities, and the likely duration of those sub-processing activities. The Controller shall communicate its decision to the Processor within 10 Business Days of receipt of such notice. For the avoidance of doubt, this Clause 1.4.1 shall also apply to any replacement Sub Processor.

1.4.2 The terms of Clause 1.4.1 shall apply to those Sub-Processors already engaged by the Processor as at the date of this Policy, unless previously consented to by the Controller with full disclosure of all material information required by Clause 1.4.1.

1.4.3 Prior to allowing a Sub Processor authorised in accordance with Clause 1.4.1 to process any Data, the Processor shall enter into a written agreement with the Sub Processor under which the Sub Processor is obliged to comply with the terms of this Policy. The Processor remains fully liable to the Controller for any acts or omissions of any Sub Processors.

1.5 Information Provision and Data Protection Audits

1.5.1 On request and at no additional charge, the Processor shall provide to the Controller all information required by the Controller to assess the Processor's compliance with this Policy and the Data Protection Laws and, to the extent possible, all information necessary for the Controller to demonstrate the Controller's compliance with the Data Protection Laws.

1.5.2 In order that the Controller and/or its authorised representative and any Supervisory Authority may audit the Processor's compliance with the Data Protection Laws and the terms of this Policy, on request and at no additional charge the Processor shall provide the Controller with:

(a) reasonable access to all relevant information, premises, Data, employees, agents, Sub Processors and assets at all locations from which obligations of the Processor under this Policy are being or have been or should have been carried out; and

(b) all reasonable assistance in carrying out the audit,

during the term of any agreement and for 36 months after the termination of any agreement, howsoever arising, subject to the Controller giving the Processor not less than five Business Days' notice (except where such audit is required by a Supervisory Authority to which the Controller is subject).

1.6 Dealings with Supervisory Authorities

1.6.1 The Processor shall promptly provide all assistance and information which is requested by any Supervisory Authority.

1.6.2 The Processor shall immediately notify the Controller of any request that it receives from any Supervisory Authority for assistance or information, unless prohibited by relevant law.

1.7 Records

1.7.1 The Processor shall maintain records of all processing activities carried out on behalf of the Controller, including:

(a) the information described in Clause 1.5;

(b) where applicable, the name and contact details of the Data Protection Officer or representative based in the European Union or United Kingdom of the Processor and of any Sub Processors;

(c) the different types of processing being carried out (if applicable);

(d) any transfers of Data outside of the EEA or UK, including the identification of the relevant country or international organisation and any documentation required to demonstrate suitable safeguards;

(e) a description of the technical and organisational security measures referred to in Clause 1.2.3,

together, the **Records.**

1.7.2 The Records shall be in written electronic format.

1.7.3 The Processor shall provide the Records to the Controller promptly on request.

1.8 Data Subjects

On request, the Processor shall take all necessary action and provide the Controller with all reasonable assistance necessary for the Controller to comply with the Controller's obligations under the Data Protection Laws in relation to:

1.8.1 the provision of information to Data Subjects;

1.8.2 the rectification of inaccurate Data in relation to a Data Subject;

1.8.3 the erasure of a Data Subject's Data; and

1.8.4 the retrieval and transfer of the Data of a Data Subject.

In particular, the Processor must promptly notify the Controller if the Processor receives a request from a Data Subject under any Data Protection Laws in respect of any Personal Data and ensure that the Processor does not respond to such a request except upon written instructions of the Controller or as required by the Data Protection Laws.

1.9 Data Breaches

1.9.1 The Processor shall notify the Controller immediately after becoming aware of any unauthorised or unlawful processing, use of, or access to the Data, or any theft of, loss of, damage to or destruction of the Data (Security Incident) or any breach of this Policy. Failure to notify the Controller shall be deemed an irremediable material breach of contract

1.9.2 In the event of a Security Incident, the Processor shall provide the Controller with full co operation and assistance in dealing with the Security Incident, in particular in relation to:

(a) resolving any data privacy or security issues involving any Data; and

(b) making any appropriate notifications to individuals affected by the Security Incident or to a Supervisory Authority (notwithstanding that the Controller will remain responsible for and have full control of the making of any such notifications).

1.9.3 The Processor shall investigate the Security Incident in the most expedient time possible and shall then provide the Controller as soon as possible thereafter with a detailed description of the Security Incident, the type of data that was the subject of the Security Incident, and any other information that the Controller may request concerning the Security Incident.

1.9.4 The Processor shall take all steps necessary to prevent a repeat of the Security Incident and shall consult with and agree those steps with the Controller unless immediate steps need to be taken and it is impractical to consult with the Controller in that respect.

1.9.5 The Processor shall co-operate with the Controller to take such reasonable measures as directed by the Controller to assist in the investigation, mitigation and remediation of each such Security Incident.

1.10 Return or Destruction of Data

1.10.1 The Processor shall, at the Controller's discretion, destroy or return all Data to the Controller on termination of any agreement with the Controller, and shall destroy or delete all copies it holds of the Data, unless relevant local law to which the Processor is subject requires that Data to be retained.

1.10.2 The Processor shall provide written certification to the Controller that it has fully complied with Clause 1.10.1 within seven (7) Business Days of the end date.

1.11 Governing Law

1.11.1 This Policy shall be governed by and construed in accordance with the governing law specified in the Principal Agreement insofar as this is not inconsistent with Data Protection Laws.

If you would like to make a request for us to remove your data from our records then please contact us GDPR@bmeimaging.co.uk.