KM Medical Software Limited

Privacy Exhibit for Compliance with the GDPR

Dear Client: **[ ]**

As you may be aware, there have recently been some important developments in data privacy and data security laws and regulations. Of particular importance is the adoption of the General Data Protection Regulation (GDPR) by the European Commission which will be enforced effective May 25, 2018.

As a consequence of the changing regulatory landscape, and due to the adoption of GDPR and its rapidly approaching effective date, we are sending you this letter agreement in order to update certain data privacy and data security related obligations as part of your company's arrangement with the KM Medical.

Please counter-sign this letter below as well as the attached Privacy Exhibit, which will form part of the Software Licence Agreement and the Maintenance Agreements previously entered into with KM Medical (the "**Master Services Agreements"),** as your and our own agreement to our respective data privacy and data security related obligations. Additionally, included in this document are the Standard Contractual Clauses for the transfer of personal data to processors established outside the European Economic Area (the "**Standard Contractual Clauses: C-to-P Transfer**" or the "C-to-P Transfer Clauses"). The C-to-P Transfer Clauses have been incorporated into the Privacy Exhibit, so by signing the Privacy Exhibit, you are signifying your agreement to the C-to-P Transfer Clauses as well. Finally, please return a signed copy of this letter and the Privacy Exhibit to us as soon as possible.

KM Medical.
Effective Date of MSA: [ ]
Reference: KM Medical-

Thank you.

Andrew O'Donoghue

Andrew O'Donoghue
CEO, KM Medical Software Ltd

Acknowledged this ____ day of ______, 20__.

Client: ____________________

By: ______________________

Title: ______________________

KM Medical Privacy Exhibit Incorporating the Standard Contractual Clauses: C-to-P Transfer

This Client Privacy Exhibit ("**Privacy Exhibit**") forms part of the Master Services Agreement between **[   ]** as the Client and **KM Medical Software Limited** as the Supplier (the "**Agreement**"), under which the Supplier agrees to provide the Client with certain services (the "**Services**").

All capitalised terms that are not expressly defined in this Privacy Exhibit will have the meanings given to them in the Agreement.

1. DEFINITIONS

"**Personal Data**", "**special categories of data**", "**process/processing**", "**Controller**", "**Processor**", "**Data Subject**" and "**supervisory authority**" shall have the same meaning as in the Regulation.

"**C-to-P Transfer Clauses**" means the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries approved by EC Commission Decision of 5 February 2010 as set out in Schedule 1 to this Privacy Exhibit.

"**Data Protection Laws**" means the Regulation, the Data Protection Act 1988 and the Data Protection Act 2003, any successor thereto, and any applicable European Union or Member State law relating to the data protection or privacy of individuals.

"**Regulation**" means Directive 95/46, and any subsequent regulation, including Regulation (EU) 2016/679 of the European Parliament and the Council (General Data Protection Regulation).

"**Regulator**" means the data protection supervisory authority which has jurisdiction over the Client's or Supplier's processing of Personal Data.

"**Sub-processor**" means any processor engaged by the Supplier or by any other sub-processor of the Supplier, which agrees to receive from the Supplier, or from any other sub-processor of the Supplier, Client Personal Data exclusively with the intention for processing activities to be carried out on behalf of the Client and in accordance with its instructions, the terms of the Agreement, the Privacy Exhibit and the terms of the written subcontract, to include the following specific sub-processors:

Google Inc., Google Ireland Limited, Google Commerce Limited, Google Asia Pacific Pte. Ltd., or Google Australia Pty Ltd for a period up to and including 05.06.2018 for the purposes of provision of email services.

2. DETAILS OF THE PROCESSING ACTIVITIES

2.1 Client shall be the Controller and Supplier shall be the Processor regarding the Personal Data processed by Supplier on Client's behalf ("**Client Personal Data**") under the Agreement.

2.2 The details of the processing activities to be carried out by the Supplier on behalf of the Client under the Agreement and in particular the special categories of data where applicable, are specified in Appendix 1 of Schedule 1.

3. OBLIGATIONS OF THE SUPPLIER

The Supplier agrees:

3.1 to process Client Personal Data only:

(a) on behalf of Client and in accordance with its documented instructions unless otherwise required by European Union or European Member State law to which the Supplier is subject;

(b) for the sole purpose of carrying out the Services or as otherwise instructed by Client, and not for the Supplier's own purposes or other commercially exploitation except in the legitimate interest of the Supplier, in accordance with section 6 f of the GDPR, or any other applicable Data Protection Laws. This provision shall not apply to anonymised DDoS and traffic statistics that may be collected as long as such data cannot be attributed directly or in combination with other data to Client's Personal Data; and

(c) in compliance with this Privacy Exhibit; and

(d) in an encrypted and anonymised manner as necessary while in transit and storage and in accordance with the current state of the art encryption technology as available in the commercial marketplace

3.2 if it is legally required to process Client Personal Data otherwise than as instructed by Client, Supplier shall notify Client before such processing occurs, unless the Data Protection Law requiring such processing prohibits the Supplier from notifying Client on an important ground of public interest, in which case it shall notify Client as soon as that Data Protection Law permits it to do so.

3.3 that it has implemented and will maintain appropriate technical and organisational measures to protect Client Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access and, in particular, where the processing involves the transmission of data over a network, against all other unlawful forms of processing. Having regard to the state of the art and cost of their implementation, the Supplier agrees that such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of Client Personal Data to be protected and will at a minimum include those measures described in Appendix 2 of Schedule 1.

3.4 that protective devices are set up for ensuring the integrity and the authenticity of Client's Personal Data, especially the state of the art protective devices against malware and similar security attacks.

3.5 that it has implemented measures to prevent Client Personal Data from undergoing any unwanted degradation or deletion without having a copy immediately usable;

3.6 that it has a business continuity plan which includes measures to reduce unavailability of the services in the event of a lasting incident or security breach, and which includes service levels and maximum recovery response and resolution time charter to face any crisis scenario;

3.7 that it will treat all Client Personal Data as confidential information and not disclose such confidential information without Client's prior written consent except:

(a) to those of its personnel who need to know the confidential information in order to carry out the Services; and

(b) where it is required by a court to disclose Client Personal Data, or there is a statutory obligation to do so, but only to the minimum extent necessary to comply with such court order or statutory obligation.

3.8 to take reasonable steps to ensure that its personnel who have access to the Personal Data:

(a) are both informed of the confidential nature of the Client Personal Data and obliged to keep such Client Personal Data confidential; and

(b) are aware of and comply with the Supplier's duties and their personal duties and obligations under this Privacy Exhibit.

3.9 that it will promptly, and at least within 36 hours, notify Client about:

(a) any instruction which, in its opinion, infringes applicable law;

(b) any actual or suspected security breach, unauthorised access, misappropriation, loss, damage or other compromise of the security, confidentiality, or integrity of Client Personal Data processed by Supplier or a sub-processor ("**Security Breach**");

(c) any complaint, communication or request received directly by the Supplier or a sub-processor from a Data Subject and pertaining to their Personal Data, without responding to that request unless it has been otherwise authorised to do so by Client; and

(d) any change in legislation applicable to the Supplier or a sub-processor which is likely to have a substantial adverse effect on the obligations in this Privacy Exhibit.

3.10 that upon discovery of any Security Breach, it shall:

(a) immediately take action to prevent any further Security Breach; and

(b) provide Client with full and prompt cooperation and assistance in relation to any notifications that Client is required to make as a result of the Security Breach.

3.11 to provide Client with full and prompt cooperation and assistance in relation to any complaint, communication or request received from a Data Subject, including by:

(a) providing Client with full details of the complaint, communication or request;

(b) where authorised by Client, complying with a request from a Data Subject in relation to their Client Personal Data within the relevant timescales set out by applicable law and in accordance with Client’s instructions;

(c) providing Client with any Client Personal Data it holds in relation to a Data Subject, if required in a commonly-used, structured, electronic and machine-readable format;

(d) providing Client with any information requested by Client relating to the processing of Client Personal Data under this Privacy Exhibit;

(e) correcting, deleting or blocking any Client Personal Data; and

(f) implementing appropriate technical and organisational measures that enable it to comply with this paragraph 3.10.

3.12 to provide Client with full and prompt cooperation and assistance in relation to any data protection impact assessment or regulatory consultation that Client is legally required to make in respect of Client Personal Data.

3.13 to appoint, and identify to Client, an individual to support the Client in monitoring compliance with this Privacy Exhibit, and to make available to Client upon request all information and evidence necessary to demonstrate that the Supplier is complying with its obligations under this Privacy Exhibit.

3.14 that it shall maintain a list of sub-processors that may Process the Personal Data of Supplier's Clients, and make available such list to Client. Supplier shall require all sub-processors to abide by substantially the same obligations as Supplier under this Agreement. Supplier remains responsible at all times for compliance with the terms of this Agreement by Supplier Affiliates and sub-processors. Client consents to Supplier's use of Supplier's Affiliates and sub-processors in the performance of the Services. Supplier shall inform Client of any new sub-processors Supplier intends to engage. Client may object to the engagement of any new sub-processor, but shall not unreasonably withheld its consent to such appointment.

3.15 upon request, to promptly send a copy of any data privacy, data protection (including but not limited to measures and certifications) and confidentiality portions of an agreement it concludes with a sub-processor relating to Client Personal Data to Client.

3.16 shall promptly notify Client should Supplier receive a request from a data subject to have access to Personal Data or any complaint or request relating to Client's obligations under applicable Data Protection Laws. Client is solely responsible for responding to such request unless Supplier does not inform Client of the request, and Supplier will not respond to any such data subject unless required by applicable laws or unless instructed in writing by Client to do so.

3.17 shall within 30 days of generating data relating to a Data Subject pursuant to the instructions received from the Client pursuant to the Master Services Agreement, delete such Customer Data following the transfer of such Customer Data to the Client. Customer is solely responsible for its own compliance with this aspect of the Privacy Laws and unless and until it receives consent from the relevant Data Subject concurrent with the Customer Data, then it shall also be obliged to delete such relevant Customer Data within the 30 day period. In the event that the Client engages the Supplier to provide outreach services on its behalf seeking consent or the Client receives the consent of the Data Subject to the control and processing of the Customer Data beyond the notified period, then the Supplier shall comply with the further instructions of the Client in respect of such processing pursuant to the other provisions of this Privacy Exhibit

4. LIABILITY

4.1 The Supplier shall remain fully liable to Client for any sub-processors' processing of Client Personal Data under the Agreement.

5. INTERNATIONAL DATA TRANSFER

5.1 The Client expressly agrees and consents to Personal Data being processed pursuant to the Master Services Agreement which shall be processed within and outside of the European Economic Area (the "EEA") by

Supplier. The following are the countries in which such data may be processed: a) United States of America; b) Vietnam and c) Singapore.

5.2 Supplier agrees to comply with all applicable Data Protection Laws, and where relevant, the C-to-P Transfer Clauses in its capacity as the processor whereby the Client will be regarded as the Data Exporter and the Supplier will be regarded as the Data Importer.

5.3 The C-to-P Transfer Clauses may be varied or terminated only as specifically set out in the C-to-P Transfer Clauses.

5.4 In the event of inconsistencies between the provisions of the C-to-P Transfer Clauses and this Privacy Exhibit or other agreements between the parties, the C-to-P Transfer Clauses shall take precedence. In the event that the C-to-P Transfer Clauses are amended, replaced or repealed by the European Commission or under Data Protection Laws, the parties shall work together in good faith to enter into any updated version of the C-to-P Transfer Clauses or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with Data Protection Laws.

6. INDEMNITY

6.1 The Supplier agrees to indemnify and keep indemnified and defend at its own expense Client against reasonable costs, claims, damages or expenses incurred by Client or for which Client may become liable due to any failure by the Supplier or its employees or agents to comply with any of its obligations under this Privacy Exhibit to an aggregate limitation of €1,500,000 in respect of all any and claims. Supplier shall not be liable in respect of any obligations which by their nature and pursuant to the Master Services Agreement are the compliance obligations of the Client, including the obligation of the Client to seek consent to the control and processing of Customer Data. The Client agrees to indemnify and keep indemnified and defend at its own expense Supplier against reasonable costs, claims, damages or expenses incurred by the Supplier, which the Supplier may become liable due to any failure by the Client or its employees or agents to comply with any of its obligations under this Privacy Exhibit to an equivalent limitation to that stated in respect of the Supplier herein.

7. ALLOCATION OF COSTS

7.1 Each party shall perform its obligations under this Privacy Exhibit at its own cost.

8. TERM AND TERMINATION OF THE SERVICES

8.1 The parties agree that Client Personal Data will be processed by the Supplier for the duration of the Services under the Master Services Agreement.

8.2 The parties agree that upon termination of the Services in so far as they relate to Client Personal Data, the Supplier and all sub-processors shall, at the choice of Client, return all Client Personal Data and the copies thereof to Client, or securely destroy all Client Personal Data and certify to Client that it or they have done so, unless a European Union or European Member State law to which the Supplier or a sub-processor are subject prevent the Supplier or sub-processor from returning or destroying all or part of the Client Personal Data. In such a case, the Supplier confirms that it will maintain the confidentiality of Client Personal Data and will not actively process Client Personal Data anymore, and will arrange the return and/or destruction of the Client Personal Data as requested by Client when the legal obligation to not return or destroy the information is no longer in effect.

9. Records and Proofs

9.1 Supplier will keep records concerning its security, and organisational technical measures as well as records on any security incident affecting Client’s Personal Data. Such records will be made available in a standard format immediately exploitable, upon Client’s reasonable written request in the course of a security check or in the framework of an audit.

10. Term, Portability and Reversibility and Survival

10.1 This Exhibit is attached to and part of the Master Services Agreement previously executed with Client, and shall remain in full force as long as such agreement remains in full force. In order to ensure portability of the Personal Data, and should the agreement be terminated for any reason, Supplier shall, within five (5) days of Client’s request, make available Client’s Personal Data in a standard format.

10.2 Survival. Any terms of this Exhibit which by their nature should survive the termination of this Exhibit shall survive such termination.

11. Miscellaneous

11.1 In the event of inconsistencies between the provisions of this Privacy Exhibit and other agreements between the parties, the provisions of this Privacy Exhibit shall prevail with regard to the parties' data protection obligations relating to Client Personal Data. In cases of doubt, this Privacy Exhibit shall prevail, in particular, where it cannot be clearly established whether a clause relates to a party's data protection obligations.

11.2 Should any provision or condition of this Privacy Exhibit be held or declared invalid, unlawful or unenforceable by a competent authority or court, then the remainder of this Privacy Exhibit shall remain valid. Such an invalidity, unlawfulness or unenforceability shall have no effect on the other provisions and conditions of this Privacy Exhibit to the maximum extent permitted by law. The provision or condition affected shall be construed either: (a) to be amended in such a way that ensures its validity, lawfulness and enforceability while preserving the parties' intentions, or if that is not possible, (ii) as if the invalid, unlawful or unenforceable part had never been contained in this Privacy Exhibit.

11.3 Any amendments to this Privacy Exhibit shall be in writing duly signed by authorised representatives of the parties hereto.

On behalf of the data exporter:
Name (written out in full):
Position:
Address:

Signature: ____________________

On behalf of the data importer:
Name (written out in full): Andrew O'Donohgue
Position: VP Operations, KM Medical
Address: Suite 9, South Terrace Medical Centre,
Infirmary Road, Cork, Ireland

Signature: Andrew O'Donoghue

SCHEDULE 1
Standard Contractual Clauses: C-to-P Transfer

1. DEFINITIONS

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. DETAILS OF THE TRANSFER

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 of Schedule 1 which forms an integral part of the Clauses.

3. THIRD-PARTY BENEFICIARY CLAUSE

3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6.1 and 6.2, Clause 7, Clause 8.2, and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. OBLIGATIONS OF THE DATA EXPORTER

The data exporter agrees:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 of Schedule 1;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5. OBLIGATIONS OF THE DATA IMPORTER

The data importer agrees:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 of Schedule 1 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 of Schedule 1 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. LIABILITY

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 6.1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 6.1 and 6.2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 8.2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

11. Sub-processing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in Clause 6.1 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 11.1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES

12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer confirms that it will ensure the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor confirm that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 12.1.

On behalf of the data exporter:
Name (written out in full):
Position:
Address:

Signature: ______________________

On behalf of the data importer:
Name (written out in full): Andrew O'Donohgue
Position: VP Operations, KM Medical
Address: Suite 9, South Terrace Medical Centre,
Infirmary Road, Cork, Ireland

Signature: Andrew O'Donoghue

APPENDIX 1 OF SCHEDULE 1
DESCRIPTION OF THE TRANSFERS (CONTROLLER TO PROCESSOR)

This Appendix forms part of the Transfer Clauses and must be completed and signed by the Parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The Data Exporter is **[   ]**

Data importer

The Data Importer is **KM Medical Software Limited.** The Data Importer provides medical practice management software as well as additional services required by the Controller pursuant to the Master Services Agreement, in the course of which it processes certain personal data as a processor.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

1. Current, former, prospective employees;
2. name, address, telephone number, e-mail address, PPSN, Insurance identification or policy number;
3. ethnic origin;
4. religious or other beliefs of a similar nature where relevant to consent to procedures
5. physical or mental health or condition
6. data concerning health;
7. sex life;
8. trade or employment category.

Categories of data

The personal data transferred concern the following categories of data (please specify):

1. Employees’ names and contact information, including addresses, emails and phone numbers.
2. patient, patient’s dependent, spouse, relative;
3. medical data;

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

1. ethnic origin;
2. religious or other beliefs of a similar nature where relevant to consent to procedures;
3. physical or mental health or condition;
4. data concerning health;
5. sex life;

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

> The personal data will be used to permit access to the KM Medical Platform by both Controller, Controller employees and patients of the controller.
>
> To facilitate the provision of practice management software pursuant to the Agreements in place between the Controller and the Processor and provision of practice administration by the Controller
>
> Collection, recording, storage, adaptation or alteration, retrieval, use, combination, erasure, destruction of all data provided by the Controller and/or patients of the Controller to the Processor pursuant to Controller instructions.

Specific Data Export Notes:

For the period 23.05.2018 until 05.06.2018 email will be exported outside of the EU due to use of Google servers. This arrangement is governed by the standard contractual clauses [Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council 2010/87/EU]. As and from 05.06.2018 email will be hosted on servers within the EU.

Transcription Services are provided by Processor Staff in India via a portal. The unit and staff in India are ISO 27001 certified. This transfer is not to a third party company, only to staff of the Processor based in India.

Appendix 2 of Schedule 1

Technical and Organisational Security Measures

This Appendix 2 forms part of the Transfer Clauses and summarises the technical, organisational and physical security measures implemented by the parties in accordance with Clauses 4(d) and 5(c).

In addition to any data security requirements set forth in the Agreement, Supplier shall comply with the following:

Physical Access Control *Unauthorised persons shall be prevented from gaining physical access to premises, buildings or rooms where personal data processing systems are located.* The processor has implemented the following controls :		**Implemented? (Yes / No)**
1.	The processor prevents unauthorised individuals from gaining access to the processor's premises.	Yes
2.	The processor restricts access to data centres / rooms were data servers are located.	Yes

System Access Control *Data processing systems must be prevented from being used without authorisation.* The processor has implemented the following controls :		**Implemented? (Yes / No)**
1.	The processor implements measures to prevent unauthorised personnel from accessing data processing systems.	Yes
2.	The processor provides dedicated user IDs for every authorised personnel accessing data processing systems for authentication purposes.	Yes
3.	The processor assigns passwords to all authorised personnel for authentication purposes.	Yes
4.	The processor ensures that all data processing systems are password protected to prevent unauthorised persons accessing any personal data: (a) after boot sequences; and (b) when left unused for a short period.	Yes
5.	The processor ensures that access control is supported by an authentication system.	Yes
6.	The processor has implemented a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password, and requires the regular change of passwords.	Yes
7.	The processor ensures that passwords are always stored in encrypted form.	Yes
8.	The processor implements a proper procedure to deactivate user accounts when a user leaves the processor (or processor function).	Yes
9.	The processor implements a proper process to adjust administrator permissions when an administrator leaves the processor (or processor function).	Yes

Data Access Control *Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and personal data must not be read, copied, modified or removed without authorisation in the course of processing or use and after storage.* The processor has implemented the following controls:		**Implemented?** **(Yes / No)**
1.	The processor ensures that personal data cannot be read, copied, modified or removed without authorisation during processing or use and after storage.	Yes
2.	The processor grants data access only to authorised personnel and assigns only the minimum data permissions necessary for those personal to fulfil their duties.	Yes
3.	The processor ensures that the personnel who use the data processing systems can access only the data to which they have a right of access.	Yes
4.	The processor restricts access to files and programs based on a "need-to-know-basis”.	Yes
5.	The processor stores physical media containing personal data in secured areas.	Yes
6.	The processor has measures in place to prevent use/installation of unauthorised hardware and/or software.	Yes
7.	The processor has established rules for the safe and permanent destruction of data that are no longer required.	Yes

Data Transmission Control *Personal data must not be read, copied, modified or removed without authorisation during transfer or storage and it shall be possible to establish to whom personal data was or is transferred.* The processor has implemented the following controls:		**Implemented?** **(Yes / No)**
1.	The processor encrypts personal data during any transmission.	Yes
2.	The processor prevents removal of personal data from the processor’s business computers or premises for any reason (unless data exporter has specifically authorised such removal for business purposes).	Yes

Input Control *The processor shall be able to examine and establish whether and by whom personal data have been entered into data processing systems, modified or removed.* The processor has implemented the following controls :		**Implemented?** **(Yes / No)**
1.	The processor has implemented controls to log administrators' and users' data processing activities.	Yes
2.	The processor permits only authorised personnel to enter, modify and remove personal data within the scope of their duties.	Yes

Job Control *Personal data being processed in the performance of a service for a controller shall be processed solely in accordance with the Master Services Agreement in place between the controller and the processor and in accordance with the instructions of the controller.* The processor has implemented the following controls :		**Implemented? (Yes / No)**
1.	The processor ensures that personal data is not used for any reasons other than for the purposes it has been contracted to perform or as otherwise instructed by the controller.	Yes
2.	The processor implements measures to ensure staff members and contractors process personal data strictly in accordance with contractual requirements and controller instructions.	Yes

Availability Control *Personal data shall be protected against accidental destruction or loss.* The processor has implemented the following controls :		**Implemented? (Yes / No)**
1. 2.	The processor creates back-up copies of personal data stored in protected environments. The processor has in place contingency plans or business recovery strategies.	Yes Yes
3.	The processor implements controls to use only authorised business equipment to perform the services.	Yes
4.	The processor ensures secure disposal of documents or data carriers containing personal data.	Yes
5.	The processor has implemented network firewalls to prevent unauthorised access to systems and services.	Yes

Organisational Requirements *The internal organisation of the processor shall meet the specific requirements of data protection. In particular, the processor shall take technical and organisational measures to avoid the accidental mixing of personal data.* The processor has implemented the following controls :		**Implemented? (Yes / No)**
1.	The processor has designated a data protection officer (or a responsible person for ensuring compliance with data protection requirements if a data protection officer is not required by law)	Yes
2.	The processor has obtained the written commitment of the employees to maintain confidentiality	Yes
3.	The processor has trained staff on data privacy and data security	Yes
4. 5.	The processor undertakes regular audits to ensure its compliance with data protection requirements. The processors platform is ISO 27001 certified.	Yes Yes