# AMS Med Technology Limited

# And

# [Company/Licensee Name]

# Software Licence and Services Agreement

# &

# Data Processing Agreement

**This Agreement is dated the [INSERT DATE] day of [MONTH, YEAR].**

**This Agreement** is made on the [INSERT DATE] day of [MONTH, YEAR];

**BETWEEN:**

**AMS Med Technology Limited**, a company incorporated in Ireland (Company Registration Number: 671538), having its registered office at 1, Cleve Business Park, Monahan Road, Cork, T12 DY6W (**"Licensor"**).

AND

**[INSERT COMPANY/LICENSEE NAME]**, a company incorporated in the United Kingdom (**[INSERT COMPANY REGISTRATION NUMBER]**), having its registered office at **[INSERT REGISTERED COMPANY ADDRESS]** (**"Licensee"**)

The Licensor and the Licensee are each a **"Party"** and together the **"Parties"**.

**RECITALS:**

**A.** AMS has developed a digital occupational health Software as a Service (SaaS) platform called 'MedApp' ("the Software") which it makes available to its Licensees that helps Licensees' manage their occupational health processes and workflows.

**B.** **[INSERT COMPANY/LICENSEE NAME]** wishes to utilise the Software.

**C.** AMS has agreed to grant and **[INSERT COMPANY/LICENSEE NAME]** has agreed to receive a licence to use the Software in accordance with the terms of this Software Licence and Data Processing Agreement ("the Agreement").

**D.** Any definition used in this Agreement shall be the definition as incorporated in this Agreement, unless expressly amended in this Agreement or stated to be a new definition.

**IT IS AGREED:**

## 1. Definitions

In this Agreement, the following words shall have the following meanings:

'**AMS**' means AMS Med Technology Ltd.

**'Agreement'** means this Software Licence and Data Processing Agreement between the Licensor and the Licensee regarding use of the Software;

**'Audit'** is an investigation to ensure the Licensee or Licensee's Client is utilising the Software as agreed;

**'Authorised Users'** are those employees and independent contractors of the Licensee who are authorised by the Licensee to use the AMS Medapp software platform;

'**Business Day'** means Monday to Friday inclusive, excluding weekends and public or bank holidays in the Republic of Ireland;

**'Confidential Information'** means information of commercial value and includes the terms of this agreement and in particular, pricing.

'**Effective Date'** is the date that the Agreement comes into effect;

**'Licensee's Client(s)'** means Licensee(s)/client(s) of the Licensor (AMS) that have entered into an agreement with the Licensor (AMS) that enables the Licensee's Client(s) to use the Software;

'**Normal Business Hours'** is 9.00am to 5.00pm local Irish time during each Business Day;

**'MedApp Platform'** is the web-based digital Software as a Service (SaaS) solution owned by the Licensor that is used to enable the Licensee to carry out the licenced software services.

**'Software'** means the Medapp Platform that is being licensed pursuant to the terms of this Agreement

'**The Term'** means the duration of the term specified in this Agreement

**'Virus'** is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.

**'Production'** is the live version of the software that is used to store the Licensee's real data. This is distinct from any other "test" versions of the software that is made available to the licensee.

## 2. Grant of Licence

**2.1.** In consideration of the payment of €1.00 (one Euro) (the receipt and sufficiency of which is hereby acknowledged by AMS), AMS hereby grants to the Licensee a non-exclusive, non-transferable, non-sublicensable, revocable licence, limited to use by Authorised Users solely for the Licensee's internal purposes to use the Software during the Term subject to and in accordance with the terms and conditions set out in this Agreement.

## 3. Rights, Obligations and Covenants of the Licensee

**3.1.** The Licensee has the right to use all functionality of the Software that has been outlined and agreed in the final proposal document submitted.

**3.2.** AMS agrees to provide the agreed functionality at the outset to the Licensee. In the event that the Licensee requires additional functionality to be included AMS will charge the Licensee to build the new modules into the Software. AMS has the right to not build in new functionality if it is not in the best interest of AMS.

**3.3.** The Licensee shall permit AMS to audit (including on site and/or remotely) the Licensee's use of the Platform in order to establish the name and password of each Authorised User and verify use of the Platform. Such audit may be conducted no more than once per quarter, at AMS expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with the Licensee's normal conduct of business.

**3.4.** The Licensee will ensure that any employee that has left the company will have his or her account disabled.

**3.5** The Licensee agrees that it will not access, store, distribute or transmit any viruses, or any material during the course of its use of the Services that:

- **a)** is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;
- **b)** depicts sexually explicit images;
- **c)** facilitates sexually explicit images;
- **d)** promotes unlawful violence;
- **e)** is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability, or any other illegal activity;
- **f)** causes damage or injury to any person or property; or facilitates illegal activity.

**3.6** Title to all intellectual property, trade secrets, and other proprietary rights in or related to the Software is and will remain the exclusive property of AMS. This is inclusive of any new development or features on the software platform after the date of this agreement.

**3.7** The Licensee agrees to not attempt to copy, duplicate, distribute, reverse-engineer or modify any portion of the Software.

**3.8** The Licensee shall not access all or any part of the Services (i.e., the structure, design and functionality) and documentation for the purpose of building a product or service that competes with the Software.

**3.9** The Licensee shall use all reasonable measures to prevent any unauthorised access to, or use of, the Software platform in the event of any such unauthorised access or use, promptly notify AMS.

**3.10** The Licensee shall and does permit AMS to anonymise and aggregate (a) the Licensee data, (b) monitor and analyse and use such anonymised and aggregated data for purposes such as provision of statistical and market data, (c) analyse use of the services, (d) use anonymised data for secondary research or clinical audit purposes where such anonymised data does not originate in personal data for which explicit consent for anonymisation is required.

**3.11** That the Licensee shall fully indemnify and hold harmless AMS against all liabilities, losses, damages, costs (including legal and or professional costs) of any kind arising from any grossly negligent or fraudulent act, error or omission caused by the Licensee whilst using the Software platform e.g., the Licensee inputs an incorrect result or measurement into the Software platform resulting in an erroneous test result.

**3.12** In the event of there being a dispute between the Parties, that they shall first seek to resolve the dispute through good-faith negotiations. If failing to resolve in that manner, the dispute shall be submitted to mediation. If mediation does not resolve the dispute within 30 days, either party may pursue remedies available at law.

**3.13** In the event that the Licensee plans to terminate the relationship with AMS, the Licensee will notify AMS in writing at least 30 days before the end of the Term of the Agreement, that the Agreement shall terminate effective upon the expiry of the relevant Term.

**3.14** In the event that AMS plans to terminate the relationship with the Licensee, AMS will notify the Licensee in writing, at least 30 days before the end of the Term that the Agreement shall terminate effective upon the expiry of the Term.

**3.15** If either party terminates the relationship by giving 1 months' notice, AMS will provide all data to the Licensee in a logically structured database export (.sql) file. This file can be transferred to Licensee or another software supplier.

**3.16** In the event that the Licensee goes into liquidation, AMS will step in and work directly with the Licensee's Client(s) in supporting the Software platform and reporting capability. If this is to arise, AMS will support and invoice the client directly based on the terms agreed between the Licensee and the Licensee's Client(s).

**3.17** In the event that there is a proposed change in control of the Licensee, the Licensee must seek the consent of AMS, failing which AMS may terminate the Agreement. Such consent is not to be unreasonably withheld.

## 4. Rights, Obligations and Covenants of AMS

**4.1** Defined Uptime Percentage (Service Availability and Uptime)

AMS will use commercially reasonable endeavours to make MedApp available with an Uptime Percentage of not less than 99.5% during each calendar year ("Uptime Commitment").

"Uptime Percentage" means the percentage calculated as:

$$\frac{\text{Total Minutes in the Year} - \text{Downtime Minutes}}{\text{Total Minutes in the Year}} \times 100$$

"Downtime" means the total number of minutes during which the SaaS Platform is unavailable to all Users, excluding Permitted Downtime.

"Permitted Downtime" means:

- Planned or Scheduled Maintenance carried out during the maintenance window of 6.00pm to 9.00am Irish Time or such times as AMS providers require, of which AMS will endeavour to provide advance notice in accordance with this Agreement;
- Emergency or unscheduled maintenance required to address security, legal, or operational risks;
- Unscheduled maintenance performed within Normal Business Hours in reaction to a software issue discovered in production that is impacting core software functionality that requires an urgent fix via a patch/hotfix production release;
- Downtime or unavailability caused by factors outside of AMS's reasonable control, including failures of third-party networks, utility services, hosting providers, internet/telecommunications services, act of God, war, riot, malicious damage or compliance with any law or government order;
- Customer systems, integrations, or misuse of the SaaS Platform.

Service Availability Measurement Method:

- Service availability shall be measured using AMS's internal monitoring systems, which may include automated uptime monitoring tools, server logs, and transaction-level checks.
- Availability shall be assessed at the application layer and shall be deemed unavailable only where MedApp is materially inaccessible to all Users.

- Partial outages, performance degradation, or unavailability affecting individual Users or specific non-core features shall not constitute Downtime unless otherwise expressly agreed in writing.
- AMS's records relating to availability and Downtime shall be conclusive in the absence of manifest error.

**4.2** AMS will as part of its services provide the Licensee with AMS standard Licensee support response and resolution target services (phone, email and/or ticketing system) during Normal Business Hours as follows:

| Incident Severity Level | Description | Initial Response Time | Target Resolution Time |
|---|---|---|---|
| **Level 1 - Critical** | Issue severely impacting core functionality with no workaround options available to perform such core functions. | 1 hour | 1 day |
| **Level 2 - High** | Issue severely impacting functionality but not preventing the operation of core functions. | 2 hours | 2 days |
| **Level 3 - Medium** | Issue impacting functionality with minor impact to performance. | 4 hours | 4 days |
| **Level 4 - Low** | Issue with only visual non-functional impact. | 4 hours | 8 days |

"Response Time" means the time from receipt of a valid support request to acknowledgement by AMS.

"Resolution Time" means the time until the incident is resolved or a reasonable workaround is provided.

All response and resolution times are **targets, not guarantees**, and do not apply where delays are caused by licensee acts or omissions.

**4.3** Escalation Procedures and Incident Escalation

Where an Incident is not resolved within the applicable target Resolution Time, the Customer may request escalation in accordance with the following procedure:

1. First Escalation: Client Relationship Manager
2. Second Escalation: Software Programme Director
3. Final Escalation: Managing Director

Escalation requests must be made through AMS's designated support channels and shall include relevant incident references and business impact details.
The Supplier shall keep the licensee reasonably informed of progress during escalated Incidents.

### 4.4 Service Credits or Remedies

Where MedApp fails to meet the Uptime Commitment in a given calendar year, the Licensee may be entitled to a service credit calculated as a percentage of the annual license fee for the MedApp service, as set out below:

| Yearly Uptime | Service Credit |
|---|---|
| < 99.5% and ≥ 99.0% | 5% |
| < 99.0% and ≥ 98.0% | 10% |
| < 98.0% | 15% |

Service credits:

- Are the licensee's sole and exclusive remedy for failure to meet the Uptime Commitment;
- Must be claimed in writing within 30 days of the end of the relevant calendar year;
- Shall be applied as a credit against future fees and are not refundable or redeemable for cash.

No service credits shall be available in respect of Downtime caused by Permitted Downtime.

## 5. Services (Custom Development, Software solutions and configuration)

**5.1.** Subject to the terms and Condition set out above, the Licensee has agreed to purchase and AMS has agreed to supply the services on the commercial terms set out herein.

## 6. Configuration/Implementation/Onboarding Fee, and Recurring Licence Fee

**6.1.** There is a configuration/implementation/onboarding fee for AMS to configure, implement and onboard MedApp for the licensee based on what is described and agreed in the final proposal document. The Licensee will pay AMS for this fee upfront along with a recurring annual license prior to configuration/implementation/onboarding planning.
The invoice will be issued on execution of this agreement and payment is required within 30 days of the invoice issue date.
See **Schedule 1** for the relevant configuration/implementation/onboarding fee.

**6.2.** AMS will charge the Licensee a recurring annual licence fee for the use of the software on an annual basis.
The invoice will be issued on execution of this agreement and payment is required within 30 days of the invoice issue date.
See **Schedule 2** for the relevant recurring annual licence fee.

**6.3.** The fees above will include support services required by the Licensee to include 1.5 day's training, with phone and email/online ticket support throughout the duration of the Agreement.

**6.4.** All prices quoted in this Agreement are exclusive of V.A.T which shall be added to AMS invoices at the appropriate rate if applicable.

## 7. Term

**7.1.** The Initial Minimum Term of this Agreement shall be for 3 years (the "**Term**").

**7.2.** The renewal Date shall be 1 year after the first licence fee invoice is issued. Invoices for year 2 and year 3 will be issued on the anniversary of the previous year's invoice issue date.

**7.3.** The agreement will automatically renew annually upon expiry of the initial term, unless you tell us that you do not want to renew by providing notice as required in the Rights, Obligations and Covenants of the Licensee.

**7.4.** Upon expiry of the Initial Term and on each Renewal Term thereafter, the Fees payable under this Agreement may be increased by AMS by written notice to the Licensee.

## 8. Variation

**8.1.** The Parties may expressly agree in writing to any variation of the provisions of this Agreement by way of a supplemental agreement, which agreement shall be interpreted in conjunction with this Agreement.

## 9. Invalidity and Severability

**9.1.** If any provision of this Agreement shall be found by any court or administrative body of any competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect the other provisions of this Agreement and all provisions not affected by such invalidity or unenforceability shall remain in full force and effect. Both Licensee and Licensor hereby agree to attempt to substitute for any invalid or unenforceable provision a valid or enforceable provision which achieves to the greatest extent possible the economic, legal and commercial objectives of the invalid or unenforceable provision.

## 10. Territory

**10.1.** The territory for this Agreement is the Republic of Ireland and the United Kingdom.

## 11. Governing Law and Jurisdiction

**11.1.** This Agreement will be governed and construed in accordance with the laws of Ireland, and the Parties hereby submit to the exclusive jurisdiction of the Irish courts.

### 12. Data Protection Provisions

Data Protection provisions to govern the processing of personal data have been agreed upon between Parties in the form of a Data Processing Agreement which forms part of this Software Licence and Services Agreement.

## Schedule 1 – Configuration, Implementation and Onboarding fee

**[TO BE INSERTED]**

## Schedule 2 – Recurring Annual Licence fees

**[TO BE INSERTED]**

## Software License and Services Agreement Signatures Section

**Signed on behalf of [INSERT COMPANY NAME] (By its Authorised Signatory)**

*Signature:* _____

*Name:*_____

*Title:*_____

*Date:* _____

**Signed on behalf of AMS Med Technology Ltd (By its Authorised Signatory)**

*Signature:* _____

*Name:*_____

*Title:*_____

*Date:* _____

# Data Processing Agreement

This Data Processing Agreement ("**Agreement**") forms part of the Software Licence Agreement known herein as the "**Principal Agreement**") between

1. **AMS Med Technology Limited**, a company incorporated in Ireland (Company Registration Number 671538), having its registered office at 1, Cleve Business Park, Monahan Road, Cork T12 DY6W (**"Processor"**);

and

2. **[INSERT COMPANY NAME]** a company incorporated in the United Kingdom **([INSERT COMPANY REGISTRATION NUMBER])**, having its registered office at [**INSERT REGISTERED ADDRESS**] (hereinafter "**the Company**").

hereinafter also referred to collectively as: "**the Parties**" and individually as "**a Party**";

**WHEREAS**

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

**IT IS AGREED AS FOLLOWS:**

## 1. Definitions and Interpretation

**1.1** Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

**1.1.1** "Agreement" means this Data Processing Agreement and all Schedules to the Data Processing Agreement.

**1.1.2** "Company Personal Data" means any Personal Data Processed by the Processor, or a Sub-processor, on behalf of Company pursuant to or in connection with the Principal Agreement.

**1.1.3** "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.

**1.1.4** "EEA" means the European Economic Area.

**1.1.5** "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

**1.1.6** "GDPR" means EU General Data Protection Regulation 2016/679.

**1.1.7** "Reasonable" refers to the standard and behaviour that is deemed appropriate in the ordinary course of business. Such standards shall be construed, and where possible, determined in accordance with relevant guidance published by the Data Protection Commission.

**1.1.8** "Services" means the consultation, software development, data processing and data storage services the Processor provides.

**1.1.9** "Sub-processor" means any entity appointed by or on behalf of the Processor to process Company Personal Data on behalf of the Processor in connection with the Agreement.

**1.1.10** "Third Country" shall mean a location outside of the European Economic Area (EEA).

**1.2** The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

## 2. Processing of Company Personal Data

**2.1** the Processor shall:

**2.1.1** comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

**2.1.2** not Process Company Personal Data other than on the relevant Company's documented (digital or written) instructions.

**2.2** The Company instructs the Processor to process Company Personal Data.

**2.3** The Company Personal Data processed will include Personal Data, and Special Categories of Data, specifically medical data, as captured in Appendix 1.

## 3. Processor Personnel

**3.1** The Processor shall take Reasonable steps to ensure the reliability of any employee, agent or contractor of their own or of any Sub-processor who may have access to the Company Personal Data.

**3.2** The Processor shall ensure in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Processor or Sub-processor .

**3.3** The Processor shall ensure that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality, as applicable.

## 4. Security

**4.1** Taking into account the state of the art technology, 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, the Processor shall in relation to the Company Personal Data

implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

**4.2** In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

Further information regarding security information is included in Appendix 2.

## 5. Sub-processing

**5.1** The Processor shall not appoint (or disclose any Company Personal Data to) any Sub-processor unless such Sub-processor can provide assurance of appropriate technical and organisational measures over data processing activities, where such assurance will be documented in Appendix 1, the Sub-processor table.

**5.2** Parties agree that Sub-processors will only process the Company Personal Data on the instructions of the Processor and the Processor will put in place a legal agreement in writing to govern the sub-processing.

**5.3** Before appointing a Sub-processor, the Processor will obtain assurances from any Sub-processors processing the Company Personal Data, that they will have in place appropriate technical and organisational measures, and all measures pursuant to Article 32 of the GDPR, to protect the confidentiality of the Personal Data and to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

**5.4** Further information regarding Sub-processors is included in Appendix 1, including information on recognised Certifications relating to required measures.

**5.5** Where the Processor changes or appoints Sub-processors, the Processor will amend the Sub-processor table in Appendix 1 and issue changes to the Company in the form of a 'Notice of Amendment to Appendix 1'.

## 6. Data Subjects and Rights

**6.1** Where the Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data, the Processor shall notify the Company in writing within 72 hours.

**6.2** The Processor shall ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Processor responds to the request.

## 7. Personal Data Breach

**7.1** The Processor shall investigate and report on any suspected incident or breach involving Company Personal Data according to the Processor internal breach management process in alignment with the Company internal breach management process.

**7.2** Where the Company requires, the Processor shall not withhold agreement to an integrated breach management process to be formulated and presented by the Company. And, where such is agreed upon, it shall be attached hereto as an Appendix.

**7.3** The Processor shall notify the Company without undue delay, but no later than 24 hours, upon the Processor becoming reasonably aware, of a Personal Data Breach affecting Company Personal Data, providing the Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

**7.4** Such notification shall include as a minimum:

**7.4.1** description of the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned,

**7.4.2** the name and contact details of the Processor's Data Protection Officer, Privacy Officer, or other relevant contact from whom more information may be obtained,

**7.4.3** describe the estimated risk and the likely consequences of the Personal Data Breach, and

**7.4.4** describe the measures taken or proposed to be taken to address the Personal Data Breach.

**7.5** The Processor shall co-operate with the Company and take Reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

## 8. Data Protection Impact Assessment and Prior Consultation

The Processor shall provide Reasonable assistance to the Company with any Data Protection Impact Assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Company reasonably considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Processor.

## 9. Deletion or return of Company Personal Data

**9.1** Where there is a cessation of any Services involving the Processing of Company Personal Data, and the Processor has been informed of a cessation date or date has arisen through termination processes, both Parties agree that the final 10 business days preceding the cessation date will be dedicated to the deletion of Company Personal Data.

**9.2** As such, the Processor commits to using the final 10 business days preceding the cessation date to ensuring the deletion of all copies of the Company Personal Data being processed for the provision of the Services under cessation.

**9.3** Where Parties agree to details of deletion and return, such arrangements shall be attached hereto as an Appendix.

## 10. Audit Rights

**10.1** Subject to this section 10, the Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Processor.

**10.2** Upon request of the Company, in accordance with provisions herein, the Processor will allow, for the purposes of audit and, where confidentiality permits, access to data processing facilities, data files and documentation used for processing, reviewing, auditing and/or certifying (or any independent or impartial inspection agents or auditors, selected by the Company and not reasonably objected to by the Processor) to ascertain compliance with the warranties and undertakings in this Agreement, with Reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Processor.

**10.3** The Company shall give at least 30 days' written notice of its intention to audit, including specific details on the scope of the audit and any required evidence.

**10.4** Evidence will include but is not limited to, provision of the Processor's procedure and process documents which demonstrate that the Processor is complying with Data Protection Law and has clear and relevant security technology and processes in place.

**10.5** The Company and the Processor shall agree upon a Reasonable time limit for the audit.

**10.6** The Company shall conduct an audit during normal business hours and not more than once every three years.

**10.7** The Company shall take all Reasonable measures to prevent material business interruption to the Processor.

**10.8** Parties shall agree a Reasonable hourly fee chargeable by the Processor, should the audit extend beyond the agreed upon Reasonable time limit.

**10.9** Where the audit causes material business interruption to the Processor, the Processor reserves the right to charge a Reasonable fee to cover the aforementioned material business interruption.

**10.10** Such an audit is subject to the confidentiality provisions of the Principal Agreement.

## 11. Data Transfer

**11.1** Data Transfers are catalogued in Appendix 1.

**11.2** If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Processor should be satisfied that an adequate Data Protection regime exists in the Third Country.

**11.3** The Processor shall seek to legitimize Data Transfers under Adequacy Decisions or Binding Corporate Rules.

**11.4** Where the Processor cannot legitimize the Data Transfer under an Adequacy Decision or the existence of Binding Corporate Rules, the Processor shall ensure that the Data Transfer is legitimized through the inclusion in Sub-processor agreements of EU approved Standard Contractual Clauses for the transfer of personal data.

**11.5** Where the Processor authorizes, facilitates, or performs a Data Transfer, the Processor will amend the Sub-processor table in Appendix 1 and issue changes to the Company in the form of a 'Notice of Amendment to Appendix 1'.

## 12. Duration

This Agreement shall remain in force until the Software Licence Agreement which forms part of this document is terminated.

## 13. Confidentiality

Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party

except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

## 14.Liability and Indemnity

**14.1** The Processor will not be liable for any claim brought by a Data Subject arising from any action by the Processor to the extent that such action resulted directly from the Company's instructions.
**14.2** The Processor agrees to indemnify, keep indemnified and defend at its own expense the Company against all costs, claims, damages or expenses incurred by the Company or for which the Company may become liable due to any failure by the Processor or its employees, subcontractors or agents to comply with any of its obligations under this Agreement and/or the Data Protection Legislation.
**14.3** Except as provided for above, both Parties shall indemnify each other for any monetary fine or penalty imposed on one by the Supervisory Authority that results from the other's breach of its obligations under this Agreement.

## 15.General Terms

**15.1** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

**15.2** The Company warrants and represents that the Processor's expected use of the Personal Data for the purposes described within this agreement and as specifically instructed by the Company will comply with the Data Protection Legislation.

**15.3** The Company warrants that it has determined the purposes and means of the processing.

**15.4** The Company warrants that where required, consent, including explicit consent, has been obtained before commencing processing the Company Personal Data in the application and system provided under the Principal Agreement.

**15.5** The Processor warrants that it will comply with all applicable law including Applicable Data Protection Law in its performance of this Agreement.

**15.6** The Processor warrants and represents its employees, sub processors, 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.

**15.7** The Processor warrants and represents 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.

**15.8** The Processor acknowledges that it will inform the Company, if, in its Reasonable opinion, an instruction of the Company infringes the Applicable Data Protection Law.

**15.9** The Processor warrants that it will only process the Personal Data on the instructions of the Company as captured in the Principal Agreement and herein including arrangements regarding further instruction.

**15.10** Both parties warrant that they are capable of demonstrating compliance with the obligations of Applicable Data Protection Law.

## 13. Governing Law and Jurisdiction

**16.1** This Agreement is governed by the laws of Ireland.

**16.2** Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Ireland, subject to possible appeal to European Courts.

## 14. Resolution of Disputes with Data Subjects or The Supervisory Authority

**17.1** In the event of a dispute or claim brought by a Data Subject or the Supervisory Authority concerning the processing of the Company Personal Data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

**17.2** The parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Supervisory Authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

**17.3** Each party shall abide by a decision of the Supervisory Authority, acknowledging that such decision may be subject to appeal.

## 15. Temporary Suspension of Data Processing and Related Arrangements

**18.1** In the event that either the Processor or the Company is in breach of its obligations under this Agreement, then either the Processor or the Company may by mutual agreement captured in writing temporarily suspend the transfer of Personal Data to the Processor until the breach is repaired or the Agreement is terminated according to provisions in the Principal Agreement.

**18.2** For the sake of clarity, 18.1 coming into effect is not a denial of access to data by the Processor to the Company.

**18.3** Should 18.1 come into effect, all Company data in the application can and will be made available to the Company through another means as requested (e.g., Database dump file).

## 16. Variation of this Agreement

The parties may not modify this Agreement except to update any information in the Appendices, in which case they will inform the Supervisory Authority where required. This does not preclude the parties from adding additional commercial clauses where required and does not affect the Principal Agreement between the Company and the Processor. In cases where any conflict arises in the interpretation of these agreements, this Agreement shall take precedence in matters of Data Protection.

**IN WITNESS WHEREOF** this Data Processing Agreement is entered into with effect from the date first set out below.

***Signed on behalf of "Company Name" (By its Authorised Signatory)***

*Signature:*_____

*Name:*_____

*Title:*_____

*Date:* _____

***Signed on behalf of Processor Company – AMS Med Technology Limited***

***(By its Authorised Signatory)***

*Signature:* _____

*Name:*_____

*Title:*_____

*Date:* _____

## Appendix 1 – Description of Processing, Sub-processor, and Data Transfers

### Location of Data Processing

Primary Sub-processor: Amazon Web Services

Location: EU primary and backup data centers in Ireland.

Description of processing: Hosting of all application data.

### Data Subjects

The Company Personal Data transferred concern the following categories of Data Subjects:

- Employees and/or Representatives of the Company (system users)
- Employees of the Company
- Potential employees of the Company

Data Subjects involved in future transfers may be identified in writing through the service request system of the Processor.

### Subject Matter, Nature, and Duration of Processing

The Processor will process Personal Data as necessary to perform under the Principal Agreement for the duration of the Principal Agreement and as further instructed by the Company in its use of the platform or services. Generally, this would include creating accounts for the Company (or employees and other representatives of the Company) on the platform to allow for access to the system.

Further purpose might relate:

Where the Data Subject is an employee that is a system user of the Company:

- For the Processor to provide support services to the Data Subject.

The Purposes of future transfers may be expressed in writing through the service request system of the Processor.

### Personal Data Categories

The Company shall determine, in the main, the data processed on the system provided. Data processed will include regular Personal Data and Special Categories of Personal Data as captured in the course of the provision of services under the Principal Agreement.

## Sub-processors

| **Full Legal Name** | **Processing Activity** | **Category Processed** | **Data Points** | **Location of Processing** | **Certification** (if applicable) |
|---|---|---|---|---|---|
| Glenbeigh Records Management | Digitisation for onboarding | Regular and Special Categories of Data | All data points to be processed in application. | Ireland | ISO 27001:2013 |
| Amazon Web Services | Application, file, database cloud hosting and email out of application service provider. | Regular and Special Categories of Data | All data points including unique employee identifier, name, contact details, and health conditions. | Ireland | SOC 2 |
| Twilio | Text reminders for appointments. | Regular Personal Data | Contact details of attendee. | Ireland | SOC 2 |

## Third Country Transfers

| **Full Legal Name** | **Processing Activity** | **Transfer To** | **Basis for Transfer out of EEA** |
|---|---|---|---|
| Twilio | Text reminders for appointments. *(Optional functionality in application.)* | Ireland -> Twilio Group | Binding Corporate Rules |

## Data Protection Officer or representative details for Company and Processor

Contact points for data protection enquiries:

**AMS Data Protection Officer (DPO)**

Name: Bernadette Millar

Telephone: +353 214297686

Email: bmillar@ameds.ie

**AMS (Data Processor) authorised representative**

Name: Garry Bennett

Telephone: +353 214297686

Email: gbennett@ameds.ie

## Appendix 2 – Security Measures

### Change Controls

Processes and tools for the Secure Software Development Lifecycle (SDLC) are integrated with appropriate security check/controls and requirements, in order to ensure that new software/applications and changes to existing software/applications are designed and developed taking into consideration the requirements of embedded security.

### Data at Rest

Databases are encrypted at rest using an AES-256 encryption algorithm.

### Physical Access Controls

The MedApp databases and application is on cloud storage with a region of storage set to Europe-Ireland.  AWS standards will apply for data centres.

### System Access Controls

Unique logins are assigned to each user.

MFA is enforced on AWS account logins.

All existing AWS accounts are reviewed on an annual basis during the technology stack review. Actions are taken as a result of this review to delete users that no longer need access.

Access authorization to production environments containing personal data should be given according to the "need to know" and “least privilege” principles.

When creating a new account, or changing the password on an existing account, the user is required to enter the new password twice, both entries must be exactly the same. Passwords created must meet minimum complexity rules regarding length of password and combination of numbers, uppercase and lowercase letters.

Policies and procedures are implemented to ensure the proper identification of users and administrators accessing system components managing personal data. All users are assigned with a unique user name before allowing them to access system components or personal data.

Logic has been implemented on login and similar account access forms and process that lock user account access for a period of time when suspicious behaviour regarding that account access has been detected.

### Data Access Controls

Visibility of personal data must be limited to the sole set of information which is necessary for the single processing activities. No unnecessary personal data should be made available to users.

### Transmission Controls

Data is encrypted in transit, transferred over HTTPS / TLS 1.3 using RSA encryption SHA-256

### Input Controls

Pages and forms on MedApp that are publicly available before logging in are protected from robot inputs by the implementation of a CAPTCHA solution. The implementation is designed to be non-distributive to humans while preventing automated processes from submitting forms.

### Data Backups

MedApp uses Amazon Web Services (AWS) for application, files and database storage and backups. Backups are configured to be taken daily in the early hours of the morning (which is the period when MedApp is expected to be at its lowest level of activity). Backups are stored to a separate physical AWS data centre location. In the event of a major incident which requires data or file recovery, AMS have a disaster recovery runbook which will allow for an organized and process driven initial investigation and identification of the best course of recovery action to minimize the impact to MedApp users. A number of checkpoints are included in this recovery runbook to determine the appropriate course of action, key to such decisions are potential data loss and the application downtime (recovery execution time).

### Data Segregation

Data and files on MedApp are logically separated by the use of a company unique identifying ID value and folder permissions structure.

Each company using MedApp is assigned a specific subdomain URL, which relates to the company unique ID value; this subdomain URL can be used only by that company to access that version of MedApp (e.g., https://***company***.medapp.ie).

Each user account with access to MedApp is associated with a single company. User accounts access to files and data is limited to files assigned the company's unique identifying ID value.