**DATA PROCESSING AGREEMENT**

This Data Processing Agreement ("DPA") forms part of the relevant controlling agreement or purchase order terms and conditions ("Agreement") entered into by and between Therakos where Therakos is the Controller of Personal Data and vendor or seller (hereinafter "Vendor"), where Vendor is the Processor of Personal Data or Service Provider on behalf of Therakos.

1. Definitions.

"**Applicable Data Protection Laws**" means all applicable federal, state or foreign data privacy, data protection, and cybersecurity laws, rules and regulations to which Therakos is subject, including but not be limited to, (a) the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1789.100 et seq., its implementing regulations, and amendments, including the California Privacy Rights Act ("CPRA") ("CCPA"); (b) the EU General Data Protection Regulation 2016/679 including the applicable implementing legislation of each Member State and as amended, replaced or superseded from time to time ("GDPR"); (c) the Directive 2002/58/EC ("ePrivacy Directive"); (d) the UK Data Protection Act 2018, the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019, and any successor legislation in each case as amended from time to time ("UK GDPR"); (e) the Canadian Personal Information Protection and Electronic Documents Act (S.C. 2000, c.5) and any successor legislation ("PIPEDA"); (f) the Australian Federal Privacy Act 1988 (No. 119, 1988); (g) the Swiss Federal Act on Data Protection (FADP); and (h) any other privacy law applicable to the Processing of Personal Data under this DPA.

"**Controller**", "**Supervisory Authority**", "**Processor**", "**Personal Data Breach**" or equivalent terms are as defined in Applicable Data Protection Laws. "Controller" shall be understood to include "Business", and "Processor" shall be understood to include "Service Provider", as those terms are defined in the CCPA.

"**Data Subject**" means a natural person to whom the Personal Data belongs. "Data Subject" shall be understood to include "Consumer" as that term is defined in the CCPA.

"**Deidentified Data**" means data that originally constituted or was derived from Personal Data, but that no longer relates to an identified or identifiable Data Subject, or which otherwise no longer constitutes Personal Data.

"**Personal Data**" means any information relating to an identified or identifiable Data Subject, whether directly or indirectly, including by reference to an identification number or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed.

"**Privacy Authority**" means any competent Supervisory Authority, attorney general, or other regulator with responsibility for privacy or data protection matters with jurisdiction over the Parties and/or any of the activities conducted by the Parties.

"**Process**", "**Processing**" or "**Processed**" means any operation or set of operations, as defined in the Applicable Data Protection Laws, performed on Personal Data, whether or not by automated means, such as accessing, collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying.

"**Restricted Transfer**" means (a) where the EU GDPR applies, a transfer of Personal Data from the EEA to a recipient in a country outside of the EEA which is not subject to valid adequacy determination by the European Commission; (b) where the UK GDPR applies, a transfer of Personal Data from the UK to a recipient in a country

outside of the UK which is not based on adequacy regulations pursuant to §17 A of the UK GDPR; (c) where the FADP applies, a transfer of Personal Data from Switzerland to a recipient in a country outside of Switzerland which has not been recognized to provide an adequate level of protection by the Federal Council; (d) an onward transfer of Personal Data by Vendor to a Sub-processor; in each case, where such transfer would be prohibited by Applicable Data Protection Laws in the absence of an adequate data transfer mechanism, such as the Standard Contractual Clauses.

"**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses as set out in the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the EU and the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses for the UK for the transfer of Personal Data to third countries pursuant to the GDPR, as may be amended or replaced by the European Commission from time to time. 1. In the event of any conflicts or inconsistencies between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall control.

"**Sub-processor**" means any third party, engaged by Vendor that will Process Personal Data in relation to the Services.

2. Obligations.

2.1. Compliance with Laws and Authorities. Each Party shall comply with its obligations under Applicable Data Protection Laws with respect to any Personal Data it Processes under this DPA. Vendor shall cooperate and comply with the directions or decisions of any relevant Privacy Authority, in each case (a) solely to the extent applicable to Vendor's Processing of Personal Data, and (b) within a reasonable time so that Therakos can meet any time limits imposed by the Privacy Authority.

2.2. Data Processing. Vendor shall (i) Process Personal Data in accordance with Therakos' written instructions, unless it is obligated to do otherwise by law, in which case Vendor will notify Therakos (unless the law prohibits Vendor from doing so on important grounds of public interest), and (ii) to the extent permitted by law, promptly inform Therakos if in Vendor's opinion, Therakos' instructions violate Applicable Data Protection Laws, and in such event, Vendor must cease the Processing until Therakos provides updated Processing instructions and the non-compliance has been resolved. The nature of the Processing is described in Annex I of the SCCs, which may be amended upon agreement by both Parties.

2.3. Data Subjects' Rights. Vendor shall reasonably and timely assist Therakos in responding to Data Subjects' requests to exercise their rights under Applicable Data Protection Laws. If Vendor receives such a request directly, it shall promptly inform Therakos and not respond to the Data Subject unless instructed by Therakos in writing to do so (except to redirect the Data Subject to Therakos). Vendor shall have in place, and maintain, reasonable and appropriate processes to ensure compliance with Therakos' instructions to update, amend, correct, provide access to, cancel, or delete a Data Subject's Personal Data.

2.4. CCPA Clause. Vendor acknowledges that it has not and will not receive any monetary or other valuable consideration in exchange for its receipt of Personal Data from Therakos. Any consideration paid by Therakos to Vendor is only for Vendor's provision of the services under the Agreement. Vendor agrees to the following:

2.4.1. All Personal Data disclosed by Therakos to Vendor, or that Vendor receives or processes on Therakos' behalf, is disclosed or received only for limited and specified purposes, including for one or more "business" or "commercial" purposes as those terms are defined under the CCPA.

2.4.2. Vendor shall not sell, share, rent, release, collect, retain, use, disclose, or otherwise Process Personal Data (i) for any purpose other than providing the specified Services, or (ii) outside of the direct business relationship between Therakos and Vendor.

2.4.3. Vendor shall maintain the confidentiality of all Personal Data as required under the Agreement and subsequent Work Orders.

2.4.4. Vendor shall not combine any Personal Data Vendor receives from or on behalf of Therakos with Personal Data that Vendor receives from or on behalf of any other third party, or that Vendor collects from its own interactions with Data Subjects, provided that Vendor may combine Personal Data for a purpose expressly permitted by Applicable Data Protection Laws or if directed by Therakos.

2.4.5.To the extent Therakos discloses or otherwise makes available Deidentified Data to Vendor, or to the extent Vendor creates Deidentified Data from Personal Data, Vendor shall (a) adopt reasonable measures to prevent such Deidentified Data from being used to infer information about, or otherwise being linked to, a particular Data Subject or household; (b) publicly commit to maintain and use such Deidentified Data in a deidentified form and to not attempt to re-identify the Deidentified Data; and (c) before sharing Deidentified Data with any other Party, including Sub-processors, and contractors ("Recipients"), contractually obligate any such Recipients to comply with all requirements of this Section 2.4 (including imposing this requirement on any further Recipients). Vendor shall remain fully liable for any failure by Vendor or its employees, Sub-processors, agents, or contractors to comply with obligations relating to Deidentified Data.

3. Security Measures and Breach Notification.

3.1. Security Measures. Vendor shall maintain appropriate technical and organizational security measures designed to protect Therakos Data against a security incident in accordance with industry standard and the security measures described in the Data Security Addendum. The measures shall include identification, containment, mitigation, and remediation of a security incident. Vendor shall provide to Therakos, upon request, any additional detailed written description of such technical and organizational measures in place.

3.2. Authorized Personnel. Vendor shall ensure that anyone it authorizes to Process Therakos Data is subject to appropriate obligation of confidentiality.

3.3. Personal Data Breach Notification. Unless otherwise prohibited by Applicable Data Protection Laws, Vendor shall notify Therakos (privacy@therakos.com) without undue delay, and in any event within 24 hours, after becoming aware of a Personal Data Breach relating to Therakos Personal Data processed by Vendor on behalf of Therakos. Vendor shall promptly investigate any incidents involving Therakos data and shall use industry standard, and commercially reasonable efforts to mitigate the effects of any such Personal Data Breach in accordance with its obligations hereunder. Vendor agrees to maintain and preserve all documents, records and other data related to any Personal Data Breach. Vendor shall not, without first obtaining Therakos' prior consent, refer to, or mention, Therakos in any communication with a Privacy Authority regarding a Personal Data Breach. For avoidance of doubt, Therakos retains the right and obligation to determine, in its sole discretion, whether notification of a Personal Data Breach processed by Vendor on behalf of Therakos to Privacy Authorities, individuals, or other persons is required.

3.4. Information and Assistance. Vendor shall provide Therakos with sufficient information to allow Therakos to meet its obligations to assess and report a Personal Data Breach under Applicable Data Protection Law, which may be provided in stages as it becomes available to Vendor, and shall include the following: (a) a description of the nature of the Personal Data Breach, including details of any Sub-processors involved, the categories and numbers of Data Subjects concerned, and the categories of Therakos Data concerned; (b) the name and contact details of Vendor's relevant contact from whom more information may be obtained; (c) the likely consequences of the Personal Data Breach; and (d) the measures taken or proposed to be taken to address the Personal Data Breach. Vendor shall co-operate with Therakos and take such reasonable steps to assist in the investigation, containment, and remediation of a Personal Data Breach.

4. Sub-processors.

4.1. Prior to outsourcing any Processing of Personal Data to a Sub-processor, Vendor shall:

(a) Provide Therakos' full details of the Processing to be (including the location of the Processing). Therakos may, within ten (10) days of receipt of that notice, object to the proposed Sub-processor(s) based on reasonable data protection grounds. If Therakos objects, Vendor shall in good faith provide a commercially reasonable alternative to the Sub-processor. Where such alternative cannot be provided within thirty (30) days of Therakos' notice, notwithstanding anything in the Agreement, Therakos may, with immediate effect, terminate without penalty the portions of the Agreement that rely on the objected to Sub-processor(s).

(b) Carry out adequate due diligence before engaging a Sub-processor to ensure that it can provide the level of data protection required by this DPA, and Vendor shall enter into a written contract with the Sub-processor that contains terms no less protective than those contained in this DPA. Upon written request by Therakos, Vendor shall make a summary of the Personal Data Processing terms with Sub-processor. In case of a Restricted Transfer, Vendor shall enter into relevant Standard Contractual Clauses with the Sub-processor.

4.2. Liability for Sub-processors. Vendor shall remain fully liable for any acts, errors, or omissions of its Sub-processor, as if they were Vendor's acts or omissions. Vendor hereby expressly waives any requirement that Therakos exhaust any right, power, or remedy, or proceed against any such Sub-processors, for any obligation or performance hereunder prior to proceeding directly against Vendor. Therakos reserves the right to decide whether to proceed against either Vendor and/or Sub-processor.

4.3. Authorized Sub-processors. Without limiting the foregoing, Therakos authorizes Vendor to engage the Sub-processors specified in Annex III to the SCCs. Any changes to this list shall be immediately reported to Therakos in accordance with Section 4.1(a) at privacy@therakos.com.

5. Data Protection Impact Assessment. Vendor shall promptly assist Therakos in carrying out any data protection impact assessment or equivalent as required under Applicable Data Protection Laws. Vendor shall reasonably cooperate with Therakos to implement such mitigation actions as are reasonably required to address privacy risks identified in any such data protection impact assessment.

6. Audits.

6.1. Audit Rights. Vendor shall permit Therakos and/or its authorized agents to audit its records to the extent reasonably required to confirm that Vendor is complying with its obligations under this DPA and Applicable Data Protection Laws. If an audit or inspection reveals that Vendor materially failed to comply or properly comply, in whole or in part, with this DPA and/or any Applicable Data Protection Laws, Vendor shall immediately remedy such failure at no cost to Therakos and bear the costs of that audit or inspection. Therakos shall provide fifteen (15) days prior written notice to conduct an audit, unless Vendor has suffered a security incident, making it more urgent to request this audit.

6.2. Audit Procedures. Such audit shall: (i) be no more than once per year, unless Vendor suffered a security incident, (ii) not involve the review of Vendor's other customers' data, (iii) require any third party conducting the audit to execute a written confidentiality agreement acceptable to Vendor or otherwise be bound by a statutory or legal confidentiality obligation, (iv) not unreasonably impact in an adverse manner Vendor's regular operations.

7. Third Party Disclosure Requests.

7.1. Vendor shall inform Therakos promptly of any inquiry, communication, request or complaint relating to the Services, any Personal Data, or any obligations under Applicable Data Protection Laws from (i) any governmental, regulatory or supervisory authority, unless prohibited by applicable law; and/or (ii) any Data Subject, within three (3) business days from receiving such request, and shall provide all reasonable assistance to enable Therakos to respond to such inquiries, communications, requests or complaints and to meet applicable statutory or regulatory deadlines. Vendor shall not disclose Personal Data to any Data Subjects or third parties unless the disclosure is at Therakos' request, permitted herein, or otherwise required by law and has otherwise complied with the obligations in this Section 7.

7.2. If Vendor or a Sub-processor is required by law, court order, warrant, or other legal judicial process ("Legal Request") to disclose any Personal Data to any person or entity other than Therakos, including any national security authority or other government body, Vendor shall attempt to redirect the Legal Request to Therakos. If Vendor is unable to redirect the Legal Request, Vendor shall notify Therakos promptly and shall provide all reasonable assistance to Therakos to enable Therakos to respond or object to the Legal Requests and meet applicable statutory or regulatory deadlines. If Vendor is prohibited by applicable law from providing notice to Therakos of a Legal Request, Vendor shall exercise commercially reasonable efforts to object to, or challenge, any such Legal Request to avoid or minimize the disclosure of Personal Data. Vendor shall not, and shall procure that any Sub-processor shall not, disclose Personal Data pursuant to a Legal Request unless it is required to do so by applicable law and has otherwise complied with the obligations in this Section 7.2.

8. International Transfers of Personal Data.

To the extent the Services provided by Vendor require a transfer of Personal Data, which would be considered a Restricted Transfer under the GDPR, UK GDPR, or FADP, the Parties agree that the transfer shall be undertaken pursuant to Standard Contractual Clauses and agree to complete all relevant details in the SCC annexes as part of the Agreement where a Restricted Transfer is involved. If additional terms are required to meet the requirements for International Transfers from a specific jurisdiction, the Parties agree to negotiate in good faith to amend this Addendum to include the required terms.

8.1. EEA Transfers.

8.1.1. Controller to Processor Transfers. In connection with an EEA Restricted Transfer: Module Two (controller to processor transfers) of the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "SCCs") shall be incorporated into the DPA by reference as follows:

(a) In Clause 7, the optional docking Clause shall not apply;

(b) In Clause 9, Option 1 shall apply, and the time period for prior notice Sub-Processor changes shall be as set out in Section 4.1(a) of this DPA;

(c) In Clause 11, the optional language shall not apply;

(d) In Clause 17, Option 2 shall apply, and the SCCs shall be governed by the law of Ireland;

(e) In Clause 18(b), disputes shall be resolved before the courts of Ireland;

(f) Annex I, II and III shall be completed.

8.1.2. Processor to Controller Transfers. In connection with an EEA Restricted Transfer: Module 4 (processor to controller transfers) of the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "SCCs") shall be incorporated into the DPA by reference as follows:

(a) In Clause 7, the optional docking Clause shall not apply;

(b) Clause 17 shall state: "These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland);

(c) Clause 18 shall state "Any dispute arising from these Clauses shall be resolved by the courts of Ireland;

(d) Annex I, II and III shall be completed.

8.2. UK Transfers. In connection with a UK Restricted Transfer: the Parties agree that the transfer shall be undertaken pursuant to the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 ("UK Addendum"), which shall be incorporated into the DPA by reference as follows: The SCCs shall apply in accordance with Section 8.1 above, but as modified and interpreted by Part 2, and shall be deemed amended as specified by Part 2: Mandatory Clauses of the UK Addendum, which shall be incorporated herein by reference. Any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. In addition:

(a) Tables 1,2,3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Annex I, II and III of the SCCs;

(b) The SCCs shall be governed by the laws of England and Wales and disputes shall be resolved before the competent England and Wales courts;

(c) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "Exporter."

Vendor shall not transfer any Personal Data to another country unless the transfer complies with the Applicable Data Protection Laws.

9. Term and Termination. This DPA shall remain in full force and effect so long as: (a) the Agreement or any Work Order remains in effect; or (b) the Vendor retains any Personal Data related to the Agreement or the Services in its possession or control, including for archiving or backup purposes. The Vendor's failure to comply with the terms of this DPA is a material breach of the Agreement. In such event, Therakos may terminate the Agreement effective immediately upon written notice to Vendor without further liability or obligation.

10. Deletion of Therakos Data. Vendor shall, promptly, and in any event within thirty (30) days of the date of term or termination of Services in the Agreement, or following receipt of written notice from Therakos, (a) return all Therakos Data to Therakos; and (b) permanently and securely delete and procure the deletion of all other copies of Therakos Data Processed by Vendor or any Sub-processor. Upon completion of deletion, Vendor shall provide Therakos with a written certificate of deletion signed by an authorized officer of Vendor within five (5) Business Days. This requirement shall not apply to the extent any law requires Vendor to retain Therakos Data (including in archives or backups), but Vendor must inform Therakos in writing of (i) that retention requirement, (ii) the legal explanation for retention, and (iii) establish specific timelines for destructions upon the end of the requirements. Vendor may only use this retained Therakos Data for the required retention reason or audit purpose. In this event, the protections, and provisions of this DPA shall continue to govern such Therakos Data for as long as it is retained by Vendor, and the term of the DPA shall extend in accordance with Section 9.

11. Records. Vendor shall keep, and if requested, provide Therakos with detailed, accurate, and up-to date records regarding any processing of Personal Data it carries out for Therakos, including but not limited to, the access, control, and security of the Personal Data, approved Sub-processors and Affiliates, the Processing purposes, and any other records required by the Applicable Data Protection Laws (the "Records"). Vendor shall ensure that the Records are sufficient to enable Therakos to verify Vendor's compliance with its obligations under this DPA.

12. Indemnity; Liability. Vendor shall defend, indemnify, and hold harmless Therakos (and each of its respective officers, employees, agents, and successors, and permitted assigns), from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, cost of enforcing any right to indemnification hereunder, and cost

of pursuing any insurance providers, arising out of or in connection with (i) any material breach by Vendor (and/or by any Sub-processor) of the provisions of this DPA, (ii) Applicable Data Protection Laws, (iii) a Personal Data Breach, or (iv) any administrative fine, penalty, or sanction imposed on Therakos by a Privacy Authority arising from or attributable to Vendor's (or any Sub-processor's) failure to comply with this DPA or Applicable Data Protection Laws.. Vendor shall be fully liable for any acts or omissions of any Sub-processors as if they were Vendor's acts or omissions. In case of a Personal Data Breach, in addition to the foregoing, Vendor shall pay for or reimburse Therakos for all costs, losses and expenses relating to the cost of forensic assessments, notifications of individuals affected, credit monitoring or fraud alert services for individuals affected, and all remedies required by law or under Therakos' contractual commitments. Any limitation of liability or disclaimer set forth in the Agreement will not apply to this DPA's indemnity or reimbursement obligations.

13. Material Breach. Vendor's failure to comply with any of the provisions of this DPA shall constitute a material breach of this DPA and the Agreement. In such event, Therakos may terminate the Agreement and subsequent Work Orders effective immediately upon written notice to Vendor without further liability or obligation.

14. Severability. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

15. Amendments. The Parties may amend this DPA if reasonably required to comply with Applicable Data Protection Laws. Without limiting the foregoing, if the SCCs are superseded by new ones approved by the European Commission, the Parties agree to work together in good faith to amend this DPA in a timely manner to execute the updated SCCs.

**ANNEX I & III**

See relevant Agreement

**ANNEX II**

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

| | |
|---|---|
| Measures of pseudonymisation and encryption of personal data | All data including personal data is encrypted to 256 AES standard in transit and at rest. |
| Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services | All systems are hosted on M365 which implements the Microsoft SOC type 2 controls standard. |
| Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident | All systems are hosted on M365 which implements the Microsoft SOC type 2 controls standard. |
| Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing | All systems are hosted on M365 which implements the Microsoft SOC type 2 controls standard. |
| Measures for user identification and authorisation | Standard username and password along with Multifactor Identification are employed along conditional access to all data |
| Measures for the protection of data during transmission | All data including personal data is encrypted to 256 AES standard in transit and at rest. |
| Measures for the protection of data during storage | All data including personal data is encrypted to 256 AES standard in transit and at rest along with multi - layer redundancy on data recovery. |
| Measures for ensuring physical security of locations at which personal data are processed | Use of Brivo door access to ensure physical security of offices. |
| Measures for ensuring events logging | Use of integrated Microsoft Defender to log all events and provide tracking of responses. |
| Measures for ensuring system configuration, including default configuration | Device management is managed by Intune. |
| Measures for certification/assurance of processes and products | All systems are hosted on M365 which implements the Microsoft SOC type 2 controls standard. |
| Measures for ensuring data minimisation | All systems are hosted on M365 which implements the Microsoft SOC type 2 controls standard. |
| Measures for ensuring accountability | CTIO / CIO / CTSO is functional lead reporting to CEO. |
| Measures for allowing data portability and ensuring erasure] | All systems are hosted on M365 which implements the Microsoft SOC type 2 controls standard. |

**CYBERSECURITY ADDENDUM**

Therakos and Vendor expressly recognize and agree that the provisions of this Cybersecurity Addendum include stipulations addressed in other portions of the Agreement. Although this Cybersecurity Addendum and the other portions of the Agreement shall be read together and construed, to the extent possible, to be in concert with each other, if there is a conflict between the two, the Cybersecurity Addendum shall prevail; provided, however, that in no event shall the provisions of this Cybersecurity Addendum be deemed to eliminate, limit or otherwise diminish Vendor's obligations or commitments to Therakos under the Agreement or applicable laws.

**1. DEFINITIONS.**

Unless otherwise specified below or herein, all capitalized terms used in this Cybersecurity Addendum ("Provisions") have the same meaning as stated in the Agreement and/or as defined in the DPA:

1.1. "**Data Protection Laws**" and "**Personal Data**" have the meanings included in the DPA.

1.2. "**Governmental Authority**" means and includes all governmental, legislative, executive, judicial, quasi-judicial, and regulatory bodies, agencies, departments or entities, including data protection and supervisory authorities, and any industry-self regulatory bodies;

1.3. "**THERAKOS Data**" means any personal data, non-public information, technical/scientific data, business methods, trade secrets and know-how, confidential data, or intellectual property of THERAKOS that Vendor may create, receive, or have access to. Therakos Data also includes any and all back-up copies created;

1.4. "**THERAKOS Personal Data**" means any Personal Data that the Vendor, its employees, agents or sub-contractors process on behalf of Therakos in performing the Vendor's obligations under or in connection with the Agreement.

1.5. "**Permitted Auditor**" means Therakos' internal and external auditors, inspectors, regulators and other representatives that Therakos may designate from time to time to conduct audits on Therakos' behalf.

1.6. "**Root Cause Analysis**" is a principles-based approach to identify the underlying causes of a Security Incident.

1.7. "**Security Incident**" means any unauthorized access, exfiltration, theft, destruction, or disclosure that materially impacts the confidentiality, integrity, or availability of Therakos Data (including without limitation Therakos Personal Data) or Therakos property. A Security Incident shall include, without limitation, a ransomware attack, denial of service attack, a personal data breach (as defined in Data Protection Laws), or any incident that may require notification to any person or Governmental Authority which impacts Therakos Data or Therakos Property.

1.8. "**Software**" means all software programs and programming for which a Party is financially or operationally responsible under the Agreement (and all modifications, replacements, upgrades, enhancements, documentation, materials and media related thereto), including applications, development tools, management tools and systems software, unless a more specific reference is required by the context.

1.9. "**System(s)**" mean the hardware, software, firmware, middleware, equipment, electronics, platforms, servers, workstations, routers, hubs, switches, interfaces, data, databases, data communication lines, network and telecommunications equipment, websites and Internet-related information technology infrastructure, wide area network and other data communications or information technology equipment, owned or leased by, licensed to, or used by Vendor or its Subcontractors to process Therakos Data.

## 2. INFORMATION SECURITY REQUIREMENTS

2.1. **Written Information Security Program.** Vendor and Subcontractors to whom Therakos Data is provided shall implement, maintain and comply with a comprehensive written information security program ("**Written Information Security Program**"), which shall include reasonable and appropriate technical, organizational and security measures against the destruction, loss, or unauthorized access, disclosure, or alteration of Therakos Data in the possession of Vendor or such Subcontractors, and shall also include incident response, disaster recovery and business continuity plans and procedures. Vendor shall provide a copy of its Written Information Security Program upon request and allow Therakos to review Vendor's compliance with the program in accordance with **Section 3** herein (Right to Audit).

2.2. **Cybersecurity Standards.** The Vendor's Written Information Security Program shall comply in all material respects with the ISO/IEC 27000 series, HITRUST, or the NIST Cybersecurity Framework, as each may be modified or replaced from time to time.

2.3. **Data Encryption.** Encryption. Vendor shall: (i) encrypt all Therakos Data in transit; (ii) encrypt all Therakos Data on portable devices; (iii) encrypt Therakos Personal Data at rest; and (iv) encrypt all other Therakos Data at rest if Vendor determines doing so is consistent with reasonable security controls. The software used by Vendor to implement such encryption shall meet AES 256 or industry best practice equivalent.

2.4. **Logging**. Vendor shall generate and maintain complete and accurate logs of all events on systems and networks used to perform the Services or otherwise process Therakos Data ("**Event Logs**"), including information such as date, time, user ID, device accessed and port used. Vendor shall maintain such Event Logs in accordance with Vendor's record retention policy, and in no event less than 90 days, and Vendor shall periodically analyze the Event Logs for security related events, unusual activities and other issues, such as unsuccessful attempts to create backup copies of Therakos Data.

2.5. **Physical Security.** Vendor shall maintain physical and environmental security for each location where information will be processed or stored for Therakos with limited and restricted access to authorized individuals only. Access to Vendor facilities must be monitored and recorded for audit purposes.

2.6. **Access to Data / Access Controls.**

a. Vendor shall ensure that controls are in place to govern access to development, test, and production systems, including their supporting infrastructure.

b. Vendor must have a documented process for granting access to resources. User and administrator access rights for all applications and environments shall be granted on a need-to-know, right-to-know and time-to-know basis utilizing a least privilege model.

c. Vendor's Systems must enforce password expiration, length of password, and password complexity.

d. The identity of the user, administrator and any other person or machine that accesses Vendor's information assets must be validated by identification (unique, non-shared login id) at a minimum and due to information asset protection may require a full authentication (password or other 2 factor (token) authentication mechanism).

e. Vendor's Systems must lock the user account after a specified number of failed login attempts.

f. Vendor shall ensure that its Systems, including without limitation, its applications, network components, and other computing devices, are protected from malicious activity by implementing the appropriate controls such as anti-virus, firewalls, and intrusion prevention systems.

g. Vendor shall implement and maintain robust controls for the secure management of cryptographic keys, including the generation, secure distribution, activation, updates, storage, recovery, replacement, immediate revocation or deactivation in cases of compromise or disaffiliation, and backup or archival as necessary to support access to THERAKOS Data. Access to cryptographic keys must be strictly limited to authorized individuals only.

2.7. **Media Sanitization.** To the extent Vendor removes Therakos Data from any media under its control that is taken out of service, Vendor shall clear, purge or destroy such data in accordance with NIST Media Sanitization Guidelines. Under no circumstances shall Vendor use or re-use media on which Therakos Data has been stored for any purpose unless Vendor has verified Therakos Data has been securely removed from such media using these NIST Guidelines.

2.8. **Vulnerability Management.**

a. Vendor shall ensure that information regarding technical vulnerabilities is obtained in a timely manner using industry standard information channels, evaluated for its relevance and potential impact to the organization's assets, and appropriate measures taken to address the associated risk.

b. Vendor will apply security patches using consistent processes in a timely manner. Unless otherwise expressly agreed in writing, "timely" shall mean that Vendor shall introduce patches as soon as commercially reasonable after the release of the patch or a fix to remediate the vulnerability.

c. Vendor must monitor and record events of systems, processes and procedures for detecting vulnerabilities, security breaches, violations and suspicious activity. This includes suspicious external activity (e.g., unauthorized probes/scans or break-in attempts) and internal activity (e.g., unauthorized administrator access, changes or misuse of systems or network, or data/information mishandling).

2.9. **Penetration Testing.**

a. Vendor shall conduct penetration testing on its Systems used to store or process Therakos Data at least once a year and at Vendor's own expense. Vendor will use its best efforts to remediate all critical and high findings within 30 days of identification. Upon request, Vendor will provide a summary of each penetration test findings to Therakos, which shall include a description of the systems tested, the risks and issues identified through testing, Vendor's acceptance or remediation of risks and issues, and remediation plans and timelines.

b. Therakos may, at its sole discretion and at its own cost, conduct an annual penetration test of Vendor's Systems used to store or process Therakos Data, which may be performed by Therakos or a third party selected by Therakos. Therakos may conduct additional penetration tests if Therakos has reason to believe there has been a Security Incident, in which case Therakos may conduct additional reviews at Vendor's cost.

2.10. **Processing Locations.** Vendor and its Subcontractors shall supply or provide the Services only at or from (i) the locations identified in Annex III to the DPA, or (ii) any location approved in writing in advance by Therakos. Vendor shall obtain Therakos' prior written approval, in Therakos' sole discretion, for any proposed relocation by Vendor or its Subcontractors of the provision of Services. Vendor shall be financially responsible for all costs associated with such relocation. Vendor shall store and process and shall permit remote access by Vendor and its Subcontractors to Therakos Data only in or from (A) the locations identified in Annex III to the DPA, or (B) any other service locations approved in writing in advance by Therakos. Vendor shall not transfer Therakos Data to any other locations, or permit access from any other locations, without the direct authorization in writing by Therakos.

2.11. **Access to Systems.** If granted access to a Therakos System, the Vendor shall (i) safeguard account authentication information and not disclose it; (ii) immediately notify the **Therakos Information Security Team** at CSIRT@Therakos.com of any (x) loss or compromise of any account authentication information or (y) any observed misuse of a System; (iii) not use or attempt to use the System for any purpose beyond the scope of contracted services; (iv) adhere to copyright and licensing regulations regarding the use of all software, (v) not install any unauthorized software onto Therakos Systems; (vii) not use any unauthorized cloud service for storing, transmitting, or processing Therakos Data. All Vendor actions on Therakos Systems are subject to audit and recording in accordance with the audit provisions set forth in **Section 3** herein.

**3. RIGHT TO AUDIT**.

3.1. **Controls Audit**.

a. THERAKOS may request that Vendor cause a Type 2 AICPA Service Organization Control (SOC 1 or SOC 2) audit or an equivalent audit under such successor standard as may then be in effect (a "**Controls Audit**") to be conducted by an independent public accounting firm on a periodic or annual basis for Vendor service delivery facilities at or from which the Services and/or services similar to the Services are provided. Vendor shall confer with Therakos as to the scope and timing of each such audit and accommodate Therakos' requirements and concerns to the extent practicable. Vendor shall provide Therakos and its independent auditors with a copy of such opinion and the resulting Controls Audit report as soon as reasonably possible after the conclusion of such audit. Vendor agrees to allow Therakos and Permitted Auditors to communicate with the auditor personnel who performed the audit regarding the Controls Audit report and work papers, to the extent Vendor's agreement with its auditing firm does not prohibit such communications, including with Vendor's express consent.

b. If the Controls Audit reveals any material security deficiencies that have the potential to threaten the confidentiality, integrity or availability of Therakos Data or Therakos Property, Therakos may require Vendor to remediate some or all such deficiencies within a reasonable time frame set by Therakos.

3.2. **Therakos Audit.** Therakos, or a third party selected by Therakos, shall have the right to perform such procedures and testing as are reasonably necessary for their assessment of the operating effectiveness of Vendor's policies, procedures and internal controls (a "**Therakos Audit**") (a) once annually, (b) if a Controls Audit reveals material security deficiencies that Therakos determines have the potential to threaten the confidentiality, integrity or availability of Therakos Data or Therakos Property, or (c) if Vendor fails to remediate, to Therakos' satisfaction, deficiencies identified by Therakos through the process set forth in Section 4.1 herein.

3.3. **Remedies.** If the Controls Audit or the Therakos Audit disclose critical- or high-level security issues that pose an unacceptable risk to Therakos Data or Therakos Property, as reasonably determined by Therakos, such issues may be grounds for termination of the Agreement. If Therakos determines these issues are capable of being cured within a reasonable time frame (informed by the severity of the security threat), Therakos may provide Vendor with an opportunity to cure, which shall be communicated in writing to Vendor. If the issues are not timely cured to Therakos' satisfaction, Therakos shall notify Vendor in writing and shall have the right to immediately terminate the Agreement without further payment obligations and Vendor shall refund to Therakos a pro rata portion of any and all prepaid fees paid by Therakos for the portion of such fees applicable to the remaining period of time as of the termination date for which such prepaid amounts were paid. The rights set forth in this section shall be in addition to, and not in lieu of, any other rights which Therakos may have at law or in equity.

3.4. **Audit Costs**. Except as provided in this **Section 3**, the Controls Audit shall be conducted, and the resulting opinion and report shall be provided, at no charge to Therakos.

## 4. INCIDENT RESPONSE AND BUSINESS CONTINUITY.

4.1. **Incident Response / Business Continuity Plan**. Vendor shall develop, maintain and, when a Security Incident occurs, implement an incident response and business continuity plan ("**Incident Response Plan**"), which shall also include disaster recovery provisions. Vendor shall test its Incident Response Plan at least annually, including as may be required in the Agreement and, upon request by Therakos, share the results of such tests with Therakos. Vendor shall correct all issues identified during these tests and perform a re-test within a reasonable period of time, not to exceed 60 days from the date of discovery.

4.2. **Backup Copies.** Vendor's Incident Response Plan or Written Information Security Plan shall require Vendor to generate and maintain backup copies of all Therakos Data residing on its Systems. Vendor shall perform backup restoration testing at least annually to ensure the integrity and accuracy of backup copies of Therakos Data.

4.3. **Notification of Security Incident.** If Vendor becomes aware of an actual or attempted Security Incident, it shall promptly (and no later than 24 hours after becoming aware) notify the **Therakos Information Security Team** at CSIRT@Therakos.com.

4.4. **Response to Security Incident.** Vendor shall investigate and reasonably cooperate with Therakos on investigations by providing all necessary and appropriate information with respect to a Security Incident (including potential or attempted Security Incidents). Vendor shall take all reasonable and appropriate steps to mitigate the adverse effects of each Security Incident. Vendor shall correct, at Therakos' request and sole discretion and at no additional charge to Therakos, any destruction, loss or alteration of any Therakos Data arising from or in connection with each Security Incident. With respect to each Security Incident, Vendor, including any forensic investigators acting on its behalf, shall promptly (and in any event as soon as reasonably practical) (A) perform a Root Cause Analysis and prepare a corrective action plan, (B) provide Therakos with written reports and detailed information, including how and when such Security Incident occurred and what actions Vendor is taking to remedy such Security Incident, (C) cooperate in the investigation of such Security Incident at Therakos' request, and (D) remediate such actual, potential or attempted security breach and take commercially reasonable actions to prevent its recurrence, to the extent the actual, potential or attempted security breach underlying such Security Incident is within Vendor's or its Subcontractor's areas of control.

4.5. **Liability and Indemnification for Security Incidents.** Notwithstanding anything to the contrary elsewhere in the Agreement, in the event a Security Incident occurs due to the acts or omissions of Vendor or any of its Subcontractors in violation of its obligations under the Agreement, these Provisions and/or Data Protection Laws, the Vendor shall be liable for and indemnify Therakos against any and all claims, actions, liabilities, losses, damages and expenses (including legal expenses) incurred by Therakos as a result of the Vendor's (or its Subcontractor's) failure to comply, including without limitation, losses related to the forensic investigation of an incident, breach notification, and offers of credit monitoring for impacted individuals, costs to reasonably restore the operations of impacted Systems, claims made by third parties or Governmental Authorities and costs associated with remedying any harm or potential harm caused by any Security Incident (including costs incurred notifying Governmental Authorities, law enforcement agencies, data subjects, or other persons).

4.6. **Restoration of THERAKOS Data**. In the event that any Therakos Data is corrupted or lost or sufficiently degraded as to be unusable, Therakos shall have the option to require the Vendor, to restore or procure the restoration of the Therakos Data insofar as such is technically possible. To the extent Vendor or any of its Subcontractors is responsible for the corruption, loss or degradation of Therakos Data, Vendor shall bear the cost of, restoring such data.

4.7. **Disaster Recovery Services**. Upon the occurrence of a Force Majeure Event that constitutes a disaster under the Incident Response Plan, Vendor shall promptly implement, as appropriate, its Incident Response Plan and provide disaster recovery and business continuity services as described

in such plan. The occurrence of a Force Majeure Event shall not relieve Vendor of its obligation to implement the Incident Response Plan and provide disaster recovery and business continuity services.

5. **Conflicts**. Therakos and Vendor expressly recognize and agree that these Provisions include stipulations addressed in other portions of the Agreement. These Provisions and the Agreement shall be read together and construed, to the extent possible, to be in concert with each other. In the event there is a conflict between the Provisions and the Agreement, the Provisions shall prevail; provided, however, that in no event shall the Provisions be deemed to eliminate, limit or otherwise diminish Vendor's obligations or commitments to Therakos under the Agreement or applicable laws.