DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**Addendum**") is incorporated into and forms part of the Agreement between TAG Veterinary Support Services, LLC (d/b/a AZPetVet) or its affiliated practice ("**Company**") and **Service Provider**.

Capitalized terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms used but not otherwise defined herein shall have the meanings given to them in the Agreement. Except as expressly modified below, the terms of the Agreement shall remain in full force and effect.

The parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement.

1. DEFINITIONS.

1.1. "**Controller**" means the entity that determines the purposes and means of the Processing of Personal Data.

1.2. "**Company Personal Data**" means Personal Data Processed by Service Provider in connection with the Agreement.

1.3. "**Data Protection Laws**" means all applicable laws, rules, and regulations of any jurisdiction relating to the protection, privacy, security, integrity, confidentiality, storage, transfer, or other Processing of Personal Data, including, without limitation, United States Data Protection Laws.

1.4. "**Data Subject**" means the identified or identifiable natural person who is the subject of Personal Data.

1.5. "**Personal Data**" means any information that constitutes "personal information," "personal data," "personally identifiable information," or similar term under Data Protection Laws.

1.6. "**Process**" means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, alignment, combination, restriction, erasure, destruction or disclosure by transmission, dissemination or otherwise making available.

1.7. "**Processor**" means the entity that Processes Personal Data on behalf of a Controller.

1.8. "**Sale**" or "**Sell**" means the transfer, disclosure, dissemination, or other exchange of Personal Data for monetary or other valuable consideration.

1.9. "**Security Incident**" means any actual or reasonably suspected accidental, unauthorized, or unlawful destruction, loss, alteration, acquisition, disclosure of, or access to Company Personal Data or information systems owned, operated, or controlled by Service Provider that Process Company Personal Data.

1.10. "**Services**" means the services provided to Company under the Agreement.

1.11. "**Subprocessor**" means an entity or other natural or legal person appointed or engaged by Service Provider to Process Company Personal Data on behalf of Company under the Agreement.

1.12. "**Supervisory Authority**" means an independent competent public authority established or recognized under Data Protection Laws.

1.13. "**United States Data Protection Laws**" means: (a) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and its implementing regulations (collectively, "**CCPA**"); (b) the Virginia Consumer Data Protection Act ("**VCPDA**"); (c) the Colorado Privacy Act and its implementing regulations ("**CPA**"); (d) the Utah Consumer Privacy Act ("**UCPA**"); (e) Connecticut SB6, An Act Concerning Personal Data Privacy and Online Monitoring ("**CTDPA**"); and (f) any other applicable law or regulation related to the protection of Company Personal Data in the United States that is already in force or that will come into force during the term of this Addendum.

2. PROCESSING OF COMPANY PERSONAL DATA.

2.1. Roles of the Parties; Compliance. The parties acknowledge and agree that, as between the parties, with regard to the Processing of Company Personal Data under the Agreement, Company is a Controller and

Service Provider is a Processor. In some circumstances, the parties acknowledge that Company may be acting as a Processor to a third-party Controller in respect of Company Personal Data, in which case Service Provider will remain a Processor with respect to the Company in such event. Service Provider shall comply at all times with Data Protection Laws and will promptly notify Company in writing if Service Provider makes a determination that it can no longer meet its obligations under Data Protection Laws.

2.2. Company Instructions. Service Provider shall only Process Company Personal Data in accordance with Company's documented instructions unless otherwise required by applicable law, in which case Service Provider will inform Company of such Processing. Company hereby instructs Service Provider to Process Company Personal Data solely to provide the Services to Company pursuant to the Agreement. Service Provider shall not Sell any Company Personal Data. Service Provider will immediately notify Company if, in its opinion, an instruction of Company infringes upon Data Protection Laws.

2.3. Details of Processing. The parties acknowledge and agree that the nature and purpose of the Processing of Company Personal Data, the types of Company Personal Data Processed, the categories of Data Subjects, and other details regarding the Processing of Company Personal Data are as set forth in **Appendix 1**. The parties further acknowledge and agree that: (a) Company's disclosure of Company Personal Data to Service Provider hereunder does not constitute a Sale; and (b) Company Personal Data disclosed by Company to Service Provider is provided to Service Provider only for the limited and specified purposes set forth in the Agreement and this Addendum.

2.4. Processing Subject to the CCPA. As used in this Section 2.4, the terms "Share," "Business Purpose," and "Commercial Purpose" shall have the meanings given in the CCPA. Service Provider shall not: (a) Sell or Share any Company Personal Data; (b) retain, use, or disclose any Company Personal Data (i) for any purpose other than for the Business Purposes specified in the Agreement, including for any Commercial Purpose other than the Business Purposes specified in the Agreement, or (ii) outside of the direct business relationship between Company and Service Provider; or (c) combine Company Personal Data received from, or on behalf of, Company with Personal Data received from or on behalf of any third party, or collected from Service Provider's own interaction with Data Subjects, except to perform any Business Purpose required by the Agreement. Service Provider will comply with all applicable obligations under the CCPA and provide the same level of privacy protection to Company Personal Data as is required by the CCPA. Company has the right to take reasonable and appropriate steps to help ensure that Service Provider uses Company Personal Data in a manner consistent with Company's obligations under the CCPA. If Service Provider notifies Company of unauthorized use of Company Personal Data, including under the foregoing sentence, Company will have the right to take reasonable and appropriate steps to stop and remediate such unauthorized use. Service Provider hereby certifies that it understands the foregoing restrictions under this Section 2.4 and will comply with them.

3. CONFIDENTIALITY. Service Provider shall: (a) limit access to Company Personal Data only to those entities and individuals who need access to the relevant Company Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Data Protection Laws in the context of that entity's or individual's duties to Company; (b) ensure that Service Provider personnel who Process Company Personal Data are subject to written obligations of confidentiality or are under an appropriate statutory obligation of confidentiality with respect to such Company Personal Data; and (c) ensure the reliability for maintaining confidentiality of any entity or individual engaged or employed in the Processing of Company Personal Data on behalf of Service Provider. For the avoidance of doubt, Company Personal Data shall be considered Company's Confidential Information (as that term is defined in the Agreement).

4. SECURITY.

4.1. Security Measures. Service Provider shall implement and maintain appropriate technical, physical, and organizational measures to ensure the confidentiality, integrity, and availability of Company Personal Data in Service Provider's care, custody, or control, and to prevent Security Incidents (the "**Security Measures**"). Such Security Measures shall: (a) be at least as protective as the measures Service Provider applies to its

own similar information; (b) comply with Data Protection Laws; and (c) without limiting the generality of the foregoing, include the security controls set forth in **Appendix 2**.

4.2. Notification of Security Incident. Service Provider shall notify Company of any Security Incident without undue delay and in no event later than 24 hours after becoming aware of such Security Incident. Such notification shall include, to the extent possible (a) a description of the Security Incident, including the suspected cause, the nature of the information affected, the number and categories of Data Subjects, the impact, and the likely consequences thereof; (b) the expected resolution time (if it has not already been resolved); (c) corrective measures to be taken, evaluation of alternatives, and next steps; and (d) the name and phone number of the Service Provider representative that Company may contact to obtain further information and updates. Service Provider agrees to keep Company informed of progress and actions taken to address the Security Incident and prevent future such Security Incidents.

4.3. Security Incident Response. After becoming aware of a Security Incident, Service Provider shall, at Service Provider's sole expense: (a) promptly take steps to diligently investigate the Security Incident; (b) identify the cause of such Security Incident, minimize harm, and prevent a recurrence; (c) fully cooperate with Company in investigating the Security Incident; and (d) provide Company with all information, logs, or images reasonably requested by Company in connection with the Security Incident, including, but not limited to, all information to allow Company and each Company Affiliate to meet any obligations to report or inform of the Security Incident under Data Protection Laws and assess the risk to Company or Company Personal Data. Unless required by applicable law, Service Provider shall not notify any third party of any Security Incident without Company's prior written consent

4.4. Remediation. Without limitation of Company's other rights or remedies under the Agreement or this Addendum, following a Security Incident, Service Provider shall indemnify Company and be responsible for the following to the extent arising from the Security Incident: (a) the cost of providing notice of the Security Incident in a manner and format determined by Company, in its sole discretion, to individuals and other third parties that Company reasonably determines should be notified of the Security Incident, such as regulators, law enforcement agencies and consumer reporting agencies; (b) the cost of providing affected individuals with credit monitoring and protection services for 12 months (or longer, if required by applicable data breach notification laws); (c) the cost of any other legally-required or industry standard measures; (d) Company's attorneys' and consultants' fees directly attributable to the Security Incident; and (e) any fines, costs, assessments, or penalties directly attributable to the Security Incident. Such amounts in this Section supersede, and are not limited by, any limitations of liability provided in the Agreement.

4.5. Requests for Company Personal Data. Service Provider shall immediately notify Company in the event of any request, inquiry, or demand (including any subpoena, court order, or other legal request) relating to Company Personal Data and direct the requesting party to submit their request, inquiry, or demand directly to Company. Service Provider shall challenge any such request, inquiry, or demand on any appropriate grounds. If compelled to disclose Company Personal Data to a law enforcement agency or regulator, Service Provider shall provide reasonable assistance and cooperation to Company in order for Company to seek a protective order or other appropriate remedy prior to any such disclosure.

5. SUBPROCESSING. Subject to the requirements of this Section 5, Company generally authorizes Service Provider to engage Subprocessors that are necessary for the Processing of Company Personal Data under the Agreement. Service Provider has provided a list of all current Subprocessors at **Appendix 3.** Service Provider shall notify Company in writing of the addition or replacement of any Subprocessor not set forth in **Appendix 3** at least thirty (30) days prior to the proposed engagement. Company may object to the proposed Subprocessor by providing Service Provider written notice of such objection. Upon receiving such an objection, Service Provider shall: (a) work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; or (b) take corrective steps requested by Company in its objection. If Service Provider informs Company that such change or corrective steps cannot be made, Company may immediately terminate all or a portion of the Agreement for convenience and receive a refund of any prepaid fees. Prior to engaging any Subprocessor, Service Provider shall enter into a

written contract with such Subprocessor containing data protection obligations at least equivalent in substance to those in this Addendum.

6. **DATA SUBJECT RIGHTS**. Service Provider shall assist Company, including by implementing appropriate technical and organizational measures, insofar as this is possible, with the fulfillment of Company's obligations under Data Protection Laws to respond to requests by Data Subjects to exercise their rights under Data Protection Laws. If Service Provider receives any request, inquiry, or complaint from a Data Subject with respect to Company Personal Data, Service Provider shall notify Company within 72 hours and provide Company with full details of the request. Service Provider shall not respond to that request except on the documented instructions of Company.

7. **ASSESSMENTS AND PRIOR CONSULTATIONS**. Service Provider shall provide reasonable assistance and cooperation to Company for Company to conduct any data protection impact assessment, transfer impact assessment, or prior consultation with a Supervisory Authority under Data Protection Laws in connection with Service Provider's Processing of Company Personal Data.

8. **RELEVANT RECORDS AND AUDIT RIGHTS**. Upon Company's request, Service Provider shall promptly make available to Company all information in Service Provider's possession reasonably necessary to demonstrate Service Provider's compliance with Data Protection Laws and Service Provider's obligations set out in this Addendum. In addition to any other audit rights granted under the Agreement, Service Provider shall allow for, cooperate with, and contribute to reasonable assessments and audits, including inspections, by Company or an auditor mandated by Company ("**Mandated Auditor**"), including of any premises where the Processing of Company Personal Data takes place, in order to assess compliance with this Addendum and Data Protection Laws.

9. **DATA TRANSFERS**. During the term of the Addendum, Company Personal Data shall at all times be hosted on servers that are physically located in the United States, unless otherwise agreed in writing by the parties. Service Provider shall comply, and provide Company with commercially reasonable assistance to comply, with all applicable data privacy, security, and cross-border transfer laws, regulations, and guidelines in the country to which and from which Company Personal Data will be transferred. Service Provider shall legitimize any cross-border exchange of Company Personal Data through data transfers mechanisms approved under Data Protection Laws, such as United Kingdom- or Europe Union-approved standard contractual clauses or binding corporate rules with respect to transfers of Personal Data out of the United Kingdom or Europe Union.

10. **DELETION OR RETURN OF COMPANY PERSONAL DATA**. Following termination or expiration of the Agreement, Service Provider shall, at Company's option, delete or return Company Personal Data and all copies to Company, except to the extent retention thereof is required by applicable law. If Service Provider retains Company Personal Data pursuant to applicable law, then: (a) Service Provider shall notify Company of such retention requirement; (b) Company Personal Data may only be retained only to the extent and for such period as required by applicable law; and (c) Service Provider shall ensure the confidentiality of all retained Company Personal Data and that such Company Personal Data is only Processed as necessary for the purpose specified in the applicable laws requiring its storage and for no other purpose.

11. **INDEMNIFICATION.** Notwithstanding anything to the contrary in the Agreement and without regard to any limitations of liability contained in the Agreement, Service Provider shall indemnify and hold harmless Company and Company's Affiliates, employees, and agents from and against any and all liabilities, losses, damages, costs, and other expenses (including attorneys' and expert witnesses' costs and other legal fees) arising from or relating to Service Provider's breach of this Addendum. In the event of any third-party claim, demand, suit, or action (a "**Claim**") for which Company (or any of Company' Affiliates, employees, or agents) is or may be entitled to indemnification under this Addendum, Company may, at Company's option, require Service Provider to defend such Claim at Service Provider's sole expense. Service Provider shall not settle any such Claim without Company's express prior written consent.

12. **GENERAL TERMS**. This Addendum will, notwithstanding the expiration or termination of the Agreement, remain in effect until Service Provider's deletion or return of all Company Personal Data. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in

force. The invalid or unenforceable provision shall be either (a) amended as necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible; or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein. To the extent of any conflict or inconsistency between this Addendum and the other terms of the Agreement, this Addendum will govern. Unless otherwise expressly stated herein, the parties will provide notices under this Addendum in accordance with the Agreement, provided that all such notices may be sent via email. This Addendum will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

APPENDIX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

1. Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing are as described in the Agreement and the Addendum.

2. Nature and purpose of the Processing of Company Personal Data

The nature and purpose of the Processing are those activities reasonably required to facilitate or support the provision of the Services as described in the Agreement and the Addendum.

3. The categories of Data Subjects to whom Company Personal Data relates

The categories of Data Subjects shall be as is contemplated or related to the Processing described in the Agreement.

4. The categories of Company Personal Data

The categories of Company Personal Data Processed are those categories contemplated in and permitted by Agreement.

5. The sensitive data included in Company Personal Data

The categories of sensitive Company Personal Data Processed are those categories contemplated in and permitted by the Agreement, and may include *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*.

The restrictions or safeguards applied to such data are described in Appendix 2.

6. The frequency of Company's transfer of Company Personal Data to Service Provider:

As specified in the Agreement, which may be on a continuous basis during the Term of the Agreement.

7. The period for which Company Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:

As set forth in the Addendum or the Agreement.

8. For transfers to Subprocessors, the subject matter, nature and duration of the Processing of Company Personal Data:

As set forth in the Addendum or the Agreement.

APPENDIX 2: SECURITY MEASURES

1. **Comprehensive Written Information Security Program**. Implement, maintain and comply with written information security policies and procedures designed to protect the confidentiality, availability, integrity, and resiliency of Company Personal Data and any systems that store or otherwise process it, which are: (a) aligned with an industry-standard control framework (e.g., NIST SP 800-53, ISO 27001, SOC 2 Type 2, CIS Critical Security Controls); (b) approved by executive management; (c) reviewed and updated at least annually; and (d) communicated to all personnel with access to Company Personal Data. Assign to an individual or a group of individuals the responsibility for developing, implementing, and

managing the organization's written information security program. Regularly test, monitor, evaluate, and update the sufficiency and effectiveness of the information security program, including Security Incident response procedures.

2. **Risk Assessment**. Conduct and document information security risk assessments at least annually and whenever there is a material change in the organization's business or technology practices that may impact the privacy, confidentiality, security, integrity, availability, or resiliency of Company Personal Data or systems used to Process Company Personal Data. The risk assessment will include periodic review and assessment of risks to the organization, monitoring compliance with the organization's policies and procedures, and reporting the condition of the organization's information security and compliance to internal senior management. Risk assessments are conducted by independent third parties or internal personnel independent of those who develop or maintain the organization's information systems or information security program and results are reported to senior management.

3. **Data Collection, Retention and Disposal**. Collect only as much Company Personal Data as needed to accomplish the purpose for which the information is collected. Securely dispose of records containing Company Personal Data so that the information cannot be read or reconstructed after it is no longer needed to comply with business purposes or legal obligations. Maintain technical and organizational measures to permit the exercise of Data Subject rights in accordance with Data Protection Laws and the Agreement, including without limitation rights of data portability and erasure.

4. **Personnel Background Checks and Training**. Conduct reasonable background checks (including criminal background checks) of any personnel or third parties who will have access to Company Personal Data or relevant information systems and repeat the checks at appropriate and adequate intervals. Prohibit individuals convicted of a crime of dishonesty, breach of trust or money laundering from having access to Company Personal Data. Train personnel to maintain the confidentiality, integrity, availability, and security of Company Personal Data, consistent with the terms of the Agreement and Data Protection Laws.

5. **Vendor Management and Oversight**. Conduct reasonable due diligence and monitoring to ensure Subprocessors are capable of (a) maintaining the privacy, confidentiality, security, integrity, and availability of Company Personal Data, (b) complying with Data Protection Laws, and (c) assisting Company with complying with requests from data subjects, including without limitation requests for data portability or erasure. Regularly assess and monitor Subprocessors to confirm their compliance with applicable privacy and information security requirements and Data Protection Laws.

6. **Access Controls**. Maintain logical access controls designed to limit access to Company Personal Data and relevant information systems only to authorized personnel and third parties (e.g., granting access on a need-to-know basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access when employment terminates or changes in job functions occur).

7. **Secure User Authentication**. Maintain password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that passwords controlling access to Company Personal Data must: (a) be at least eight (8) characters in length and meet minimum complexity requirements; (b) not be stored in readable format on the organization's computer systems; (c) have a history threshold to prevent reuse of recent passwords; and (d) if newly issued, be changed after first use.

8. **Incident Detection and Response**. Maintain policies and procedures to detect, monitor, document and respond to actual or reasonably suspected Security Incidents.

9. **Pseudonymization and Encryption**. Where feasible and in accordance with the Agreement, use technical and organizational measures to pseudonymize Company Personal Data in accordance with Data Protection Laws. Apply industry standard encryption to Company Personal Data: (a) stored on any medium (i.e., laptops, mobile devices, portable storage devices, file servers and application databases); and (b) transmitted across any public network (such as the Internet) or wirelessly.

10. **Network Security**. Implement network security controls such as up-to-date firewalls, layered DMZs, updated intrusion detection/prevention systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

11. **Data Segregation**. Physically or logically segregate Company Personal Data to ensure it is not comingled with another party's data unless approved by Company.

12. **Malicious Code Detection**. Implement and maintain software that detects, prevents, removes, and remedies malicious code designed to perform an unauthorized function on, or permit unauthorized access to, any information system, including viruses, Trojan horses, worms, and time or logic bombs.

13. **Vulnerability and Patch Management**. Maintain vulnerability management and regular application, operating system and other infrastructure patching procedures and technologies to identify, assess, mitigate, and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code.

14. **Change Controls**. Prior to implementing changes to the organization's information systems, follow a documented change management process to assess the potential impact of such changes on privacy, confidentiality, security, integrity, and availability of Company Personal Data, and determine whether such changes are consistent with the organization's information security program.

15. **Off-Premise Information Security**. Maintain policies governing the security of the storage, access, transportation and destruction of records or media containing Company Personal Data outside of business premises. Monitor and document movement of records or media containing Company Personal Data.

16. **Physical Security**. Ensure physical and environmental security of data centre, server room facilities and other areas containing Company Personal Data designed to: (a) protect information assets from unauthorized physical access; (b) manage, monitor and log movement of persons into and out of facilities; and (c) guard against environmental hazards such as heat, fire and water damage.

17. **Business Continuity and Disaster Recovery**. Maintain policies and procedures for responding to and recovering from an emergency or other occurrence that can compromise the privacy, confidentiality, integrity, or availability of Company Personal Data or damage the organization's information systems.

APPENDIX 3: SUBPROCESSOR LIST

For all subprocessors Service Provider uses to provide Services under the Agreement, Service Provider shall provide the following information to Company within two (2) weeks of execution of the Agreement:

- Subprocessor Name
- Processing Purpose
- Location
- Contact Point for Data Protection Matters