Data Processing Agreement

This Data Processing Agreement (the "Agreement") between Provider (sometimes referred to as "Provider," "we," "us," or "our"), and the Client found on the applicable Master Services Agreement, Order, or Service Description (sometimes referred to as "you," or "your,") and, together with the Order, Proposal, Master Services Agreement, and other relevant Service Attachments or Descriptions, forms the Agreement between the parties the terms to which the parties agree to be bound.

The parties agree as follows:

1. Health Insurance Portability and Accountability Act ("HIPAA") Data Processing. This Agreement documents the safeguards imposed upon the parties to protect health information that is subject to the Health Insurance Portability and Accountability Act ("HIPAA"). If Provider is engaged as a "Business Associate" under HIPAA, then this Agreement shall apply to Provider's activities as a Business Associate. If HIPAA applies to Provider's activities as a Business Associate, in Order to demonstrate the parties' compliance with HIPAA, this Agreement applies to each agreement between Provider or any of Provider's Affiliates and Client or any of Client's Affiliates under which Provider engages protected health information as part of its performance.

a. DEFINITIONS

The following terms used in this Agreement have the same meanings as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific Definitions:

- Business Associate. "Business Associate" generally has the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this Agreement, means Provider.
- Covered Entity. "Covered Entity" generally has the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this Agreement, means Client.
- HIPAA Rules. "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

b. OBLIGATIONS OF BUSINESS ASSOCIATE

Business Associate agrees to:

i. Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;
ii. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;
iii. Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected

health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

iv. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;

v. Make available protected health information in a designated record set to the covered entity as necessary to satisfy covered entity's obligations under 45 CFR 164.524;

vi. Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

vii. To the extent required by regulators, maintain and make available the information required to provide an accounting of disclosures to the covered entity as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

viii. To the extent the Business Associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

ix. To the extent required by regulators, make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

c. PERMITTED USES AND DISCLOSURES

i. Business Associate may only use or disclose protected health information as necessary to perform the services set forth in the Master Services Agreement. The Business Associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the Business Associate will de-identify the information and the permitted uses and disclosures by the Business Associate of the de-identified information.

ii. Business Associate may use or disclose protected health information as required by law.

iii. Business Associate agrees to make uses and disclosures and requests for protected health information consistent with covered entity's minimum necessary policies and procedures.

iv. Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity.

v. Business Associate may disclose protected health information for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

vi. Business Associate may provide data aggregation services relating to the health care operations of the covered entity.

d. PRIVACY PRACTICES AND RESTRICTIONS

i. Covered entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information.

ii. Covered entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the

extent that such changes may affect Business Associate's use or disclosure of protected health information.

iii. Covered entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

e. PERMISSIBLE REQUESTS

Covered entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity.

2. Gramm-Leach-Bliley Act ("GLBA") Data Processing. This section documents the safeguard standards imposed to protect Client financial information subject to the Gramm-Leach Bliley Act ("GLBA"). To the extent Provider's services constitute processing of personal information governed by GLBA, these provisions shall apply.

a. DEFINITIONS

All capitalized terms in this Addendum which are not otherwise defined in this Addendum or in the MSA have the meaning set forth in Title V of the Gramm-Leach-Bliley Act (P. L. 106-102; 15 USC §6801 et seq.) and the regulations issued pursuant thereto by the Financial Institution's Functional Regulator.

b. RECEIPT OF INFORMATION

To perform its duties under the Agreement, Provider is authorized and permitted to receive, hold and, to the extent necessary, review Nonpublic Personal Information of Client in order to provide services for Client at Client's direction as provided under the MSA. Provider may further use and disclose Nonpublic Personal Information for the proper management and administration of the business of Provider.

c. OBLIGATIONS OF SERVICE PROVIDER

Provider will take reasonable steps to:

- Implement and maintain a written comprehensive information security program containing administrative, technical and physical safeguards for the security and protection of Nonpublic Personal Information and further containing each of the elements set forth in § 314.4 of the Gramm Leach Bliley Standards for Safeguarding Client Information (16 C.F.R. § 314) and the Red Flag Rules issued by the Federal Trade Commission;
- Ensure the security and confidentiality of Nonpublic Personal Information received from Client;
- Protect against any anticipated threats or hazards to the security or integrity of Nonpublic Personal Information;
- Protect against unauthorized access to or use of such information that could result in harm or inconvenience to Client;
- Ensure the proper disposal of Nonpublic Personal Information, as set forth in the MSA or in Service Attachments signed under the MSA, and
- Notify Client of any loss or breach of the security or Confidentiality of Client's Nonpublic Personal Information.

d. PERMITTED USES AND DISCLOSURES

Provider may disclose the information received by it under the Agreement only if the disclosure is required by law.

e. PERMISSIBLE REQUESTS

Client shall not request Provider to use or disclose Nonpublic Personal Information in any manner that would not be permissible Title V of the Gramm-Leach-Bliley Act (P. L. 106-102; 15 USC §6801 et seq.) and the regulations issued pursuant thereto if done by Client.

3. California Consumer and Privacy Act. This section documents the safeguard standards imposed to protect Client information subject to the California Consumer and Privacy Act ("CCPA"). To the extent Provider's services constitute processing of personal information governed by CCPA, these provisions shall apply.

a. DEFINITIONS

- **i.** "CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100 et. seq., and its implementing regulations.
- **ii.** "Client Personal Information" means any Client Data maintained by Client and processed by Provider solely on Client's behalf, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, to the extent that such information is protected as "personal information" (or an analogous variation of such term) under applicable U.S. Data Protection Laws.
- **iii.** "U.S. Data Protection Laws" means all laws and regulations of the United States of America, including the CCPA, applicable to the processing of personal information (or an analogous variation of such term).
- **iv.** "Service Provider" has the meaning set forth in Section 1798.140(v) of the CCPA.

b. Roles. The parties acknowledge and agree that with regard to the processing of Client Personal Information performed solely on behalf of Client, Provider is a Service Provider and receives Client Personal Information pursuant to the business purpose of providing the Services to Client in accordance with the Agreement.

c. No Sale of Client Personal Information to Provider. Client and Provider hereby acknowledge and agree that in no event shall the transfer of Client Personal Information from Client to Provider pursuant to the Agreement constitute a sale of information to Provider, and that nothing in the Agreement shall be construed as providing for the sale of Client Personal Information to Provider.

d. Limitations on Use and Disclosure. Provider is prohibited from using or disclosing Client Personal Information for any purpose other than the specific purpose of performing the Services specified in the Agreement, the permitted business purposes set under applicable law, and as required under applicable law. Provider hereby certifies that it understands the foregoing restriction and will comply with it in accordance with the requirements of applicable U.S. Data Protection Laws.

e. Data Subject Access Requests. Provider will reasonably assist Client with any data subject access, erasure or opt-out requests and objections. If Provider receives any request from data subjects, authorities, or others relating to its data processing, Provider will without undue delay inform Client and reasonably assist Client with developing a response (but Provider will not itself respond other than to confirm receipt of the request, to inform the data subject, authority or other third party that their request has been forwarded to Client, and/or to refer them to Client, except per reasonable instructions from Client). Provider will also reasonably assist Client with the resolution of any request or inquiries that Client receives from data protection authorities relating to Provider, unless Provider elects to object such requests directly with such authorities.

4. New York SHIELD

Provider maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of Provider's

business; (b) the amount of resources available to Provider; (c) the type of information that Provider will store; and (d) the need for security and confidentiality of such information. The Security Exhibit may be updated by Provider from time-to-time.

Provider's security program is designed to:

- Protect the confidentiality, integrity, and availability of Customer Data or Professional Services Data in Provider's possession or control or to which Provider has access;
- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Customer Data or Professional Services Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Customer Data or Professional Services Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data or Professional Services Data; and
- Safeguard information as set forth in any local, state or federal regulations by which Provider may be regulated.

Without limiting the generality of the foregoing, Provider's security program includes:

1. **Security Awareness and Training**.A mandatory security awareness and training program for all members of Provider's workforce (including management), which includes:
   a) Training on how to implement and comply with its Information Security Program;
   b) Promoting a culture of security awareness through periodic communications from senior management with employees.

2. **Access Controls**. Policies, procedures, and logical controls:
   a) To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
   b) To prevent those workforce members and others who should not have access from obtaining access; and
   c) To remove access in a timely basis in the event of a change in job responsibilities or job status.

3. **Physical and Environmental Security**. Controls that provide reasonable assurance that access to physical servers at the production data center or the facility housing Provider's SFTP Server, if applicable, is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes. These controls include:
   a) Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;
   b) Camera surveillance systems at critical internal and external entry points to the data center;
   c) Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and
   d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

4. **Security Incident Procedures**. A security incident response plan that includes procedures to be followed in the event of any Security Breach. Such procedures include:
   a) Roles and responsibilities: formation of an internal incident response team with a response

leader;
b) Investigation: assessing the risk the incident poses and determining who may be affected;
c) Communication: internal reporting as well as a notification process in the event of unauthorized disclosure of Customer Data or Professional Services Data;
d) Recordkeeping: keeping a record of what was done and by whom to help in later analysis and possible legal action; and
e) Audit: conducting and documenting root cause analysis and remediation plan.

5. **Contingency Planning**. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

a) Data Backups: A policy for performing periodic backups of production file systems and databases or Professional Services Data on Provider's SFTP Server, as applicable, according to a defined schedule;
b) Disaster Recovery: A formal disaster recovery plan for the production data center, including:
   i) Requirements for the disaster plan to be tested on a regular basis, currently twice a year; and
   ii) A documented executive summary of the Disaster Recovery testing, at least annually, which is available upon request to customers.
c) Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

6. **Audit Controls**. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information.

7. **Data Integrity**. Policies and procedures to ensure the confidentiality, integrity, and availability of Customer Data or Professional Services Data and protect it from disclosure, improper alteration, or destruction.

8. **Storage and Transmission Security**. Security measures to guard against unauthorized access to Customer Data or Professional Services Data that is being transmitted over a public electronic communications network or stored electronically. Such measures include requiring encryption of any Customer Data or Professional Services Data stored on desktops, laptops or other removable storage devices.

9. **Secure Disposal**. Policies and procedures regarding the secure disposal of tangible property containing Customer Data or Professional Services Data, taking into account available technology so that Customer Data or Professional Services Data cannot be practicably read or reconstructed.

10. **Assigned Security Responsibility**. Assigning responsibility for the development, implementation, and maintenance of its Information Security Program, including:
a) Designating a security official with overall responsibility;
b) Defining security roles and responsibilities for individuals with security responsibilities; and
c) Designating a Security Council consisting of cross-functional management representatives to meet on a regular basis.

11. **Testing**. Regularly testing the key controls, systems and procedures of its information security

program to validate that they are properly implemented and effective in addressing the threats and risks identified.

12. **Monitoring**. Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes:
    a) Reviewing changes affecting systems handling authentication, authorization, and auditing;
    b) Reviewing privileged access to Provider production systems; and
    c) Engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

13. **Change and Configuration Management**. Maintaining policies and procedures for managing changes Provider makes to production systems, applications, and databases. Such policies and procedures include:
    a) A process for documenting, testing and approving the patching and maintenance of the Service;
    b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and
    c) A process for Provider to utilize a third party to conduct web application-level security assessments. These assessments generally include testing, where applicable, for:
        i) Cross-site request forgery
        ii) Services scanning
        iii) Improper input handling (e.g., cross-site scripting, SQL injection, XML injection, cross-site flashing)
        iv) XML and SOAP attacks
        v) Weak session management
        vi) Data validation flaws and data model constraint inconsistencies
        vii) Insufficient authentication
        viii) Insufficient authorization

14. **Program Adjustments**. Provider monitors, evaluates, and adjusts, as appropriate, the security program in light of:
    a) Any relevant changes in technology and any internal or external threats to Provider or the Customer Data or Professional Services Data;
    b) Security and data privacy regulations applicable to Provider; and
    c) Provider's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

15. **Devices**. All laptop and desktop computing devices utilized by Provider and any subcontractors when accessing Customer Data or Professional Services Data:
    a) will be equipped with hard disk drive encryption;
    b) will have up to date virus and malware detection and prevention software installed with virus definitions updated on a regular basis; and
    c) shall maintain virus and malware detection and prevention software so as to remain on a supported release. This shall include, but not be limited to, promptly implementing any applicable security-related enhancement or fix made available by supplier of such software.

Definitions

"Professional Services" means consulting or professional services provided to Customer under an agreement between the parties for the provision of consulting or professional services.

"**Professional Services Data**" means electronic data or information that is provided to Provider under a Professional Services engagement with Provider for the purpose of being input into the Provider Service, or Customer Data accessed within or extracted from the Customer's tenant to perform the Professional Services.

"**SFTP Server**" means a Secure File Transfer Protocol server or its successor provided and controlled by Provider to transfer the Professional Services Data between Customer and Provider for implementation purposes.

5. General Data Protection Regulation ("GDPR")

The European General Data Protection Regulation ("GDPR") imposes specific obligations on "Processors", "Controllers", and others with regard to their vendor relationships (as defined below). GDPR requires companies to conduct appropriate due diligence on processors and to have contracts containing specific provisions relating to data protection.

If Provider is engaged in "Processing" of data, then this Addendum shall apply to Provider's activities as a "Processor". If GDPR applies to Provider's activities as a Processor, in order to demonstrate the parties' compliance with GDPR, this Addendum applies to each agreement between Provider and Client under which Provider Processes Personal Data as part of performing under that agreement ("Agreement"). If GDPR is applicable to Provider's activities, the Addendum will be effective on the last signature date set forth below ("Addendum Effective Date").

DEFINITIONS

"GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation, together with any addition implementing legislation, rules or regulations that are issued by applicable supervisory authorities. All capitalized terms in this Addendum which are not otherwise defined in this Addendum or in the Agreement have the meaning set forth in the GDPR. Words and phrases in this Addendum shall, to the greatest extent possible, have the meanings given to them in Article 4 of the GDPR. In particular:

(a) "Controller" has the meaning given to it in Article 4(7) of the GDPR: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law," but only to the extent such personal data pertains to residents of the European Economic Area ("EEA") or are otherwise subject to the GDPR.

(b) "Personal Data" has the meaning given to it in Article 4(1) of the GDPR: "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person," but only to the extent such personal data pertains to residents of the EEA or are otherwise subject to the GDPR.

(c) "Personal Data Breach" has the meaning given to it in Article 4(12) of the GDPR: "[any] 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."

(d) "Processing" has the meaning given to it in Article 4(2) of the GDPR: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"

(e) "Processor" has the meaning given to it in Article 4(8) of the GDPR: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller," but only to the extent

such personal data pertains to residents of the EEA or are otherwise subject to the GDPR.

(f) “Sub-processor” means any processor as defined in Article 4(8) of the GDPR: “[any] natural or legal person, public authority, agency or other body which processes personal data” on behalf of the Processor (including any affiliate of the Processor).

(g) “Transfer” means to disclose or otherwise make Personal Data available to a third party (including to any affiliate or Sub-processor), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means.

OBLIGATIONS OF A PROCESSOR

Technical Measures

In accordance with GDPR Article 28(1), Processor represents that it has implemented appropriate technical and organizational measures in such a manner that its Processing of Personal Data will meet the requirements of GDPR and ensure the protection of the rights of the data subjects.

Sub-processors

In accordance with GDPR Article 28(2), the Processor shall not engage any Sub-processor without prior specific or general written authorization of Client. In the case of general written authorization, the Processor shall inform Client of any intended changes concerning the addition or replacement of other Sub-processors and give Client the opportunity to object to such changes. The Processor shall also comply with the requirements for sub-processing as set forth in Article 28(4), namely that the data protection obligations set forth herein (and as may otherwise be agreed by the Processor in the Agreement) such be imposed upon the Sub-processor, so that the Processor’s contract with the Sub-processor contains sufficient guarantees that the Processing will meet the requirements of GDPR.

Processing & Security

In accordance with GDPR Article 28(3), the following terms are incorporated by reference into the Agreement:

(a) The Processor shall only process the Personal Data only (i) as needed to provide the Services, (ii) in accordance with the specific instructions that it has received from Client, including with regard to any Transfers, and (iii) as needed to comply with law (in which case, the Processor shall provide prior notice to Client of such legal requirement, unless that law prohibits this disclosure), and (iv) with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by European Union or Member State law to which Client is subject, in such case, Client will inform Provider of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(b) Processor shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) Processor shall take all security measures required by GDPR Article 32, namely:

(i) Taking into account the state of the art, 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 implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

(ii) In assessing the appropriate level of security account shall be taken in particular of the risks that are p resented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

(iii) The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process them except on instructions from

Client, unless he or she is required to do so by EEA Member State law.

(d) Taking into account the nature of the processing, Processor shall reasonably assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Client's obligation to respond to requests for exercising the data subject's rights;

(e) Taking into account the nature of processing and the information available to the Processor, Processor shall comply with (and shall reasonably assist Client to comply with) the obligations regarding Personal Data Breaches (as set forth in GDPR Articles 33 and 34), data protection impact assessments (as set forth in GDPR Article 35), and prior consultation (as set forth in GDPR Article 36);

(f) At Client's discretion, the Processor shall delete or return all the Personal Data to Client after the end of the provision of Services relating to Processing, and delete existing copies unless applicable EEA member state law requires storage of the Personal Data;

(g) The Processor shall provide Client with all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client; and

(h) The Processor shall immediately inform Client if, in its opinion, an instruction infringes the GDPR other EEA Member State data protection provisions.

Personal Data Transfers

The Processor shall not Transfer any Personal Data (and shall not permit its Sub-processors to Transfer any Personal Data) without the prior consent of Client. The Processor understands that Client must approve and document that adequate protection for the Personal Data will exist after the Transfer, using contracts that provide sufficient guarantees (such as standard contractual clauses) unless another legal basis for the Transfer exists.

Unauthorized Access & Breach Notification

The Processor will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Data. Processor will notify Client without undue delay in the event of any Personal Data Breach.

Maintenance & Availability of Records

The Processor shall maintain all records required by Article 30(2) of the GDPR, and (to the extent they are applicable to Processor's activities for Client) Processor shall make them available to Client upon request.

COMPLIANCE WITH LAWS

To the extent that GDPR applies to Provider and Client's activities under this Attachment, Provider shall comply with all data protection laws applicable to Provider in its role as a data Processor Processing Personal Data. For the avoidance of doubt, Provider is not responsible for complying with data protection laws applicable to Customer (as a data Controller) or Customer's industry. Customer shall comply with all data protection laws applicable to Customer as a data Controller.

If Provider maintains Personal Data on Provider's computers or machines, Provider will take responsibility to assist Customer with GDPR compliance at Provider's then current hourly rates.
If Customer maintains data on Customer's computers or machines, and not on Provider's machines or computers, Provider will assist Customer with GDPR compliance at Provider's then current hourly rates.

DEFENSE OF CLAIMS

Where Provider faces an actual or potential claim arising out of or related to violation of any GDPR obligations (e.g., Article 82 of the GDPR) concerning the Services, Client will promptly provide all materials and information requested by Provider that is relevant to the defense of such claim and the underlying circumstances concerning the claim.

STATEMENT OF WORK

The subject matter and duration of the Processing, the nature and purpose of the Processing, and the type of

Personal Data and categories of data subjects will be described in a statement of work, purchase order or written agreement signed by the parties' authorized representatives, which forms an integral part of the Agreement.

INSURANCE

In addition to any other insurance required under the Agreement, Client will maintain insurance coverage for privacy and cybersecurity liability (including costs arising from data destruction, hacking or intentional breaches, crisis management activity related to data breaches, and legal claims for security breach, privacy violations, and notification costs) of at least $2,000,000 US per occurrence.

TERM AND TERMINATION

(a) Term. The Term of this Agreement shall be effective as of the date signed by both parties below, and shall terminate upon the termination of the Agreement or upon the date Client terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Provider authorizes termination of this Agreement by Client, if Client determines Provider has violated a material term of the Agreement and Provider has not cured the breach or ended the violation within ten (10) business days.

(c) Effect of Termination. Upon termination of this Agreement for any reason, Provider, with respect to Personal Data received from Client, or created, maintained, or received by Provider on behalf of Client, shall:

(i) Retain only that Personal Data which is necessary for Provider to continue its proper management and administration or to carry out its legal responsibilities;

(ii) Return to Client [or, if agreed to by Client, destroy] the remaining Personal Data that the Provider still maintains in any form;

(iii) Continue to use appropriate safeguards with respect to Personal Data to prevent use or disclosure of the Personal Data, other than as provided for in this Section, for as long as Provider retains the Personal Data;

(iv) Not use or disclose the Personal Data retained by Provider other than for the purposes for which such Personal Data was retained and subject to the same conditions set forth in this Agreement; and

(v) Return to Client [or, if agreed to by Client, destroy] the Personal Data retained by Provider when it is no longer needed by Provider for its proper management and administration or to carry out its legal responsibilities.

In addition, Client's termination of this Agreement for cause constitutes good cause for Client to terminate any Service Attachments signed under the Agreement in connection with which Provider received any Personal Data from Client.

(d) Survival. The obligations of Provider under this Section shall survive the termination of this Agreement.

THIS AGREEMENT IS SUBJECT TO CHANGE UPON THIRTY (30) DAYS' PRIOR WRITTEN NOTIFICATION BY PROVIDER TO CLIENT.